Université Hadj Lakhdar-Batna

Institut d'Hygiène et Sécurité Industrielle
Laboratoire de Recherche en Prévention Industrielle

THESE

En vue de l’obtention du grade de

DOCTEUR

En Hygiène et Sécurité Industrielle
Option: Management des Risques Industriels et Environnementaux

Par

CHEBILA Mourad

Modélisation et Evaluation des Performances des Systèmes Instrumentés de Sécurité avec Prise en Compte des Incertitudes

Soutenue le 10 mai 2015 devant le jury composé de:

Djebabra Mebarek, Professeur à l’université de Batna	Président
Innal Fares, Maître de conférences à l’université de Batna	Rapporteur
Hamzi Rachida, Maître de conférences à l’université de Batna	Co-rapporteur
Nait-Said Rachid, Professeur à l’université de Batna	Examinateur
Korichi Mourad, Maître de conférences à l’université d’Ouargla	Examinateur
Hassini Abdelatif, Maître de conférences à l’université d’Oran	Examinateur

University Hadj Lakhdar - Batna

Institute of Industrial Health and Safety

Laboratory of Research in Industrial Prevention

MODELING AND EVALUATING THE PERFORMANCE OF SAFETY INSTRUMENTED SYSTEMS WITH THE CONSIDERATION OF THE ASSOCIATED UNCERTAINTIES

A thesis presented

by

Mourad Chebila

in partial fulfillment of the requirements for the degree of

Doctor

in the subject of

Industrial Health and Safety

Option: Management of Industrial and Environmental Risks

Advisory Committee:

Djebabra Mebarek, Professor at Batna University	President
Innal Fares, Associate Professor at Batna University	Advisor
Hamzi Rachida, Associate Professor at Batna University	Co-advisor
Nait-Said Rachid, Professor at Batna University	Examiner
Korichi Mourad, Associate Professor at Ouargla University	Examiner
Hassini Abdelatif, Associate Professor at Oran University	Examiner

May 2015

Abstracts

In today’s industrial facilities that are often based on the employment of the sophisticated equipments and activities as well as the highly hazardous substances, safety instrumented systems (SISs) constitute an essential layer in the process of preventing the occurrence of the dangerous events and protecting the exposed targets (e.g., human beings, environment and properties). Evaluating the performance of such safety devices is fundamental to forecast the level of their ability to perform their intended functions when required and the one of their spurious activations. The main objective of this PhD thesis is to develop a set of generalized and simplified analytical formulas for some of the widely used performance indicators of SISs, namely: average probability of failure on demand (PFD_{avg}), probability of failure per hour (PFH), average probability of failing safely (PFS_{avg}) and spurious trip rate (STR). The implementation of such purpose requires some preliminary investigation on the involved models and assumptions. Moreover, the treatment of the associated parametric uncertainty is indispensable and must be carried out in an appropriate framework.

Keywords: Functional safety, safety instrumented systems, common cause failures, reliability, partial stroking tests, uncertainty and sensitivity analysis.

ملخص

في منشآتنا الصناعية التي غالبا ما تستند على توظيف التجهيزات والأنشطة المتطورة والمعقدة فضلا عن المواد الشديدة الخطورة، تشكل أنظمة السلامة المجهزة (SIS) طبقة أساسية في عملية منع وقوع الأحداث الخطيرة وحماية الأهداف المعرضة لها (مثل البشر، البيئة والممتلكات). يعتبر تقييم أداء مثل هذه الأجهزة أمرا أساسيا للتنبؤ بمستوى قدرتها على أداء وظائفها المقصودة عند الاقتضاء بالإضافة إلى قدرتها على النشاط الزائف و الغير مرغوب فيه. الهدف الرئيسي من رسالة الدكتوراه هذه هو اقتراح مجموعة من الصيغ التحليلية المعممة والمبسطة لبعض مؤشرات الأداء المستخدمة على نطاق واسع ل SIS، وهي: متوسط احتمال الفشل على الطلب (PFD_{avg})، احتمال الفشل بالساعة (PFH)، متوسط احتمال الفشل بأمان (PFS_{avg}) ومعدل النشاط الزائف (STR). تحقيق هذا الغرض يتطلب بعض التحقيقات الأولية عن النماذج والافتراضات المستعملة. وعلاوة على ذلك، فإن معالجة عدم اليقين الحدودي المرتبطة لا غنى عنه وينبغي تنفيذه في إطاره المناسب.

كلمات مفتاحية: السلامة الوظيفية، أنظمة السلامة المجهزة، فشل بسبب مشترك، الموثوقية، اختبارات الجس الجزئية، تحليل عدم اليقين و الحساسية.

Résumé

Dans les installations industrielles d'aujourd'hui qui sont souvent fondées sur l'emploi des équipements et activités sophistiqués ainsi que les substances extrêmement dangereuses, les systèmes instrumentés de sécurité (SIS) constituent une couche essentielle dans le processus de prévention de l’occurrence des événements dangereux et protection des cibles exposés (p.ex., êtres humains, environnement et propriétés). L'évaluation des performances de ces dispositifs de sécurité est fondamentale pour la prévision du niveau de leur capacité à accomplir leurs fonctions prévues en cas de besoin et l'un de leurs fausses activations. L'objectif principal de cette thèse est de développer un ensemble de formules analytiques généralisées et simplifiées pour certains des indicateurs de performance des SIS, qui sont: la probabilité moyenne de défaillance sur demande (PFD_{avg}), probabilité de défaillance par heure (PFH), probabilité moyenne de défaillance en sécurité (PFS_{avg}) et taux de déclenchement intempestif (STR). La mise en œuvre d'un tel objectif nécessite une étude préliminaire sur les modèles et les hypothèses impliquées. De surcroît, le traitement de l’incertitude paramétrique associée est indispensable et devrait être effectué dans un cadre approprié.

Mots clés: Sécurité fonctionnelle, systèmes instrumentés de sécurité, défaillances de cause commune, fiabilité, tests sur course partielle, analyse d'incertitude et de sensibilité.

Publications

1) **Unification of Common Cause Failures' Parametric Models Using a Generic Markovian Model**. ***Mourad Chebila*** *and Fares Innal*. Journal of Failure Analysis and Prevention. Vol: 14, No: 3, pp. 426-434. 2014.
2) **Generalized Analytical Expressions for Safety Instrumented Systems' Performance Measures: PFDavg and PFH**. ***Mourad Chebila*** *and Fares Innal*. Journal of Loss Prevention in the Process Industries. Vol: 34, pp. 167-176. 2015.
3) **Comparative Study between the Beta Factor and Multiple Beta Factor Models**. ***Mourad Chebila*** *and Fares Innal*. Third International Conference on Industrial Engineering and Manufacturing (ICIEM'2014). Batna, 2014.
4) **Treatment of Uncertainty in Probabilistic Risk Assessment Using Monte Carlo Analysis**. *Fares Innal,* ***Mourad Chebila****, Mouloud Bourareche and Antar Si Mohamed*. Proceedings of the 3rd International Conference on Systems and Control. Algiers, 2013.
5) **Monte Carlo Analysis and Fuzzy Sets for Uncertainty Propagation in SIS Performance Assessment**. *Fares Innal, Yves Dutuit and* ***Mourad Chebila***. International Journal of Physical Science and Engineering, Vol: 7, No: 11, pp. 306-314. 2013.
6) **Safety and Operational Integrity Evaluation and Design Optimisation of Safety Instrumented Systems**. *Fares Innal, Yves Dutuit and* ***Mourad Chebila***. Journal of Reliability Engineering and System Safety. Vol: 134, pp. 32-50. 2015.

Acknowledgments

Alhamdulillah,

I would like to thank Dr. Fares Innal for his incessant help, enthusiasm and valuable guidance during the three years of preparation of this thesis. Honestly, I learned countless and priceless things from him. My sincere thanks also go to Dr. Rachida Hamzi for co-advising this work and, most importantly, for her immense support especially in the last year.

I would also like to express the deepest appreciation to my advisory committee’s members Pr. Mebarek Djebabra, Pr. Rachid Nait-Said, Dr. Mourad Korichi and Dr. Abdelatif Hassini for their efforts, encouragement and precious comments.

Big thanks to all the staff (professors and administrators) of the Institute of Industrial Health and Safety in Batna University.

I deeply appreciate the huge support of my dear friends Hamid, Antar, Zakaria and Assam, thank you for being there for me.

My deepest thanks are reserved to the most important people in my universe: my parents, brothers and sisters.

Thanks to everyone who contributed in any way in this thesis.

Contents

Abstracts .... **ii**
Publications .... **iii**
Acknowledgments .... **iv**
Contents .... **v**
List of Tables .... **vii**
List of Figures .... **ix**
Abbreviations .... **xii**
Introduction **1**

1. BASIC CONCEPTS' CLARIFICATION **4**
1.1 Dependability **5**
1.1.1 Threats 6
1.1.2 Attributes 7
1.1.3 Means 11
1.2 Process safety **12**
1.3 Functional safety **18**
1.4 Testing policies **23**
1.4.1 Automatic on-line diagnostic testing 23
1.4.2 Proof testing 24
1.4.3 Partial stroke testing 24
1.5 Conclusion **26**

2. QUANTIFICATION OF THE COMMON CAUSE FAILURES' CONTRIBUTION **27**
2.1 Common cause failures' parametric models **28**
2.1.1 Beta Factor model 30
2.1.2 Multiple Greek Letter (MGL) model 30
2.1.3 Alpha Factor model 30
2.1.4 Binomial Failure Rate (BFR) model 31
2.1.5 Multiple Beta Factor (MBF) model 31
2.2 Unification of the parametric models **32**
2.3 Illustrative example **33**
2.3.1 1oo4 architecture 35
2.3.2 2oo4 architecture 36
2.3.3 3oo4 architecture 37
2.3.4 4oo4 architecture 39
2.4 Quantitative comparison between the Beta Factor model and MBF model **40**
2.4.1 Three components (*N*=3) 41
2.4.2 Four components (*N*=4) 43
2.5 Conclusion **46**

3. IMPACT OF SAFE/DANGEROUS FAILURES ON SAFETY/OPERATIONAL INTEGRITY **48**

3.1 Quantitative evaluation of safe failures' impact on the safety integrity 49
3.1.1 Modeling construction 49
3.1.2 Results presentation and discussion 56
3.2 Quantitative evaluation of dangerous failures' impact on the operational integrity................................59
3.2.1 Results presentation and discussion 60
3.3 Conclusion...63

4. MODELING THE SAFETY INSTRUMENTED SYSTEMS' PERFORMANCE 64
4.1 Safety integrity related metrics 65
4.1.1 Considering the dangerous (detected/undetected) failures with proof tests 65
4.1.2 Considering the dangerous undetected failures with proof and partial stroking tests 69
4.1.3 Considering the dangerous (detected/undetected) failures with proof and partial stroking tests 74
4.2 Operational integrity related metrics 77
4.2.1 Generic Markov model for *K*oo*N* architectures (safe failures) 77
4.2.2 Extracting $PFS_{Koo\mathrm{N}}$ and STR_{KooN} from the Markov model 78
4.2.3 Results comparison 80
4.3 Conclusion...82

5. PARAMETRIC UNCERTAINTY AND SENSITIVITY ANALYSIS 83
5.1 Uncertainty analysis...84
5.1.1 Definition 84
5.1.2 Classification of uncertainty 84
5.1.3 Representation of uncertainty 86
5.2 Sensitivity analysis...93
5.2.1 Local sensitivity analysis 93
5.2.2 Global sensitivity analysis 94
5.3 Treatment of parametric uncertainty and sensitivity analysis in the context of safety instrumented systems...94
5.3.1 Case 1: All the probability distributions of all the input parameters can be defined.................................95
5.3.2 Case 2: Only bounds 98
5.3.3 Case 3: Multi-type parameters 101
5.4 Combining Monte Carlo and fuzzy sets approaches 105
5.4.1 General information 111
5.4.2 Monte Carlo simulation 111
5.4.3 Statistical analysis 111
5.4.4 Compliance measures 112
5.4.5 Sensitivity analysis..112
5.4.6 Illustrative example...113
5.5 Conclusion...117

Conclusions and perspectives 118
References 120
Appendix 130

List of Tables

Table 1.1 Reasons of the occurrence of failures in the three regions of the bathtub curve (Dhillon, 2006) 8

Table 1.2 Comparison of PSM systems (Bridges, 1994) 16

Table 1.3 Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation (IEC 61508, 2010) 22

Table 1.4 Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation (IEC 61508, 2010) 22

Table 2.1 Modification factors, C_{MooN}, based on system voting logic 31

Table 2.2 Values of the failure rates obtained by using different parametric models 34

Table 2.3 U_{avg} and w_{avg} for the 1oo4 architecture 35

Table 2.4 U_{avg} and w_{avg} for the 2oo4 architecture 36

Table 2.5 U_{avg} and w_{avg} for the 3oo4 architecture 38

Table 2.6 U_{avg} and w_{avg} for the 4oo4 architecture 39

Table 2.7 The different Q_k^m values obtained by using the two parametric models 41

Table 2.8 U_{avg} and w_{avg} for the 1oo3 architecture 41

Table 2.9 U_{avg} and w_{avg} for the 2oo3 architecture 42

Table 2.10 U_{avg} and w_{avg} for the 1oo4 architecture 43

Table 2.11 U_{avg} and w_{avg} for the 2oo4 architecture 44

Table 2.12 U_{avg} and w_{avg} for the 3oo4 architecture 45

Table 3.1 Modeling parameters 50

Table 3.2 Modeling results for the PFD_{avg} 56

Table 3.3 Modeling results for the *PFH* 57

Table 3.4 Safe failure states of each configuration 59

Table 3.5 Modeling results for the PFS_{avg} 60

Table 3.6 Modeling results for the *STR* 61

Table 4.1 PFD_{avg} and *PFH* values with DD/DU failures and PT (without CCF) 69

Table 4.2 PFD_{avg} and *PFH* values with DD/DU failures and PT (with CCF) 69

Table 4.3 PFD_{avg} values with DU failures, PT and PST (without CCF) 73

Table 4.4 *PFH* values with DU failures, PT and PST (without CCF) 73

Table 4.5 PFD_{avg} values with DU failures, PT and PST (with CCF) 74

Table 4.6 *PFH* values with DU failures, PT and PST (with CCF) 74

Table 4.7 PFD_{avg} values with DD/DU failures, PT and PST (without CCF) 77

Table 4.8 Results related to PFS_{avg} for different *K*oo*N* architectures 82

Table 4.9 Results related to *STR* for different *K*oo*N* architectures 82

Table 5.1 Triangular, Trapezoidal and Gaussian fuzzy numbers 91

Table 5.2 Data associated with the 2oo3 subsystem (probability distributions) 95

Table 5.3 PFD_{avg} and PFH of the 2oo3 subsystem (without uncertainty) 95

Table 5.4 PFD_{avg} and PFH of the 2oo3 subsystem (with uncertainty handled by MC simulation)........... 96

Table 5.5 Sensitivity analysis related to PFD_{avg} of the 2oo3 subsystem (probabilistic framework).......... 97

Table 5.6 Sensitivity analysis related to PFH of the 2oo3 subsystem (probabilistic framework) 97

Table 5.7 Data associated with the 2oo3 subsystem (intervals)... 99

Table 5.8 A priori belief mass distributions of the root nodes of the 2oo3 subsystem 99

Table 5.9 PFD_{avg} and PFH of the 2oo3 subsystem (with uncertainty handled by ENs).......................... 100

Table 5.10 Sensitivity analysis of the 2oo3 subsystem (inputs as intervals)... 101

Table 5.11 Non-exhaustive list of mathematical representations consistent with the nature of the information (Baudrit, 2005)... 102

Table 5.12 Data associated with the 2oo3 subsystem (multi-type data) 102

Table 5.13 PFD_{avg} and PFH of the 2oo3 subsystem (with uncertainty handled by PBA)....................... 103

Table 5.14 Sensitivity analysis of the 2oo3 subsystem (multi-type parameters) 104

Table 5.15 Reliability characteristics of the SIS Elements 105

Table 5.16 Obtained results from the MC approach 105

Table 5.17 Fuzzy characteristics for the SIS elements.. 107

Table 5.18 Obtained results from the fuzzy sets approach ($d\alpha$ =1E-3) 107

Table 5.19 Compliance measures related to different required SILs 109

Table 5.20 Reliability characteristics for the SIS elements... 114

Table 5.21 Obtained results from the combined approach.. 114

Table 5.22 Sensitivity measures related to the parameters of the subsystem FE 116

List of Figures

Fig. 1.1 The dependability tree (Avizienis, et al., 2004) 6
Fig. 1.2 Bathtub curve 8
Fig. 1.3 Representation of *MTTF*, *MDT*, *MUT* and *MTBF* (Villemeur, 1988) 9
Fig. 1.4 U.S. coal mining fatalities, according to (MSHA, 2013) 12
Fig. 1.5 Occupational safety vs. process safety 15
Fig. 1.6 Process safety indicator pyramid (ANSI / API RP-754, 2010) 17
Fig. 1.7 Relationship of some standards and guidelines to IEC 61508 (Smith, et al., 2004) 19
Fig. 1.8 Overall safety lifecycle (IEC 61508, 2010) 20
Fig. 1.9 Typical risk reduction methods found in process plants (IEC 61511, 2003) 21
Fig. 1.10 Failures' classification 23
Fig. 1.11: Safety loop failures sources 25
Fig. 2.1 Physical elements of a dependent event (NUREG/CR-4780, 1988) 28
Fig. 2.2 Assignment of common cause models to different classes (NEA/ CSNI/ R (92) 18, 1993) 29
Fig. 2.3 Unified Markov model for the CCF parametric models 33
Fig. 2.4 Unified Markov model for a system of four components 34
Fig. 2.5 *U* (*t*) for 1oo4 configuration 35
Fig. 2.6 *w* (*t*) for 1oo4 configuration 36
Fig. 2.7 *U* (*t*) for 2oo4 configuration 37
Fig. 2.8 *w* (*t*) for 2oo4 configuration 37
Fig. 2.9 *U* (*t*) for 3oo4 configuration 38
Fig. 2.10 *w* (*t*) for 3oo4 configuration 38
Fig. 2.11 *U* (*t*) for 4oo4 configuration 39
Fig. 2.12 *w* (*t*) for 4oo4 configuration 39
Fig. 2.13 *U* (*t*) for 1oo3 configuration 41
Fig. 2.14 *w* (*t*) for 1oo3 configuration 42
Fig. 2.15 *U* (*t*) for 2oo3 configuration 42
Fig. 2.16 *w* (*t*) for 2oo3 configuration 43
Fig. 2.17 *U* (*t*) for 1oo4 configuration 43
Fig. 2.18 *w* (*t*) for 1oo4 configuration 44
Fig. 2.19 *U* (*t*) for 2oo4 configuration 44
Fig. 2.20 *w* (*t*) for 2oo4 configuration 45
Fig. 2.21 *U* (*t*) for 3oo4 configuration 45
Fig. 2.22 *w* (*t*) for 3oo4 configuration 46

Fig. 3.1 1oo1 electrical diagram 50
Fig. 3.2 1oo1 multi-phase Markov model 50
Fig. 3.3 1oo2 electrical diagram 51
Fig. 3.4 1oo2 multi-phase Markov model 51
Fig. 3.5 2oo2 electrical diagram 52
Fig. 3.6 2oo2 multi-phase Markov model 52
Fig. 3.7 1oo2D electrical diagram 53
Fig. 3.8 1oo2D multi-phase Markov model 53
Fig. 3.9 1oo3 electrical diagram 54
Fig. 3.10 1oo3 multi-phase Markov model 54
Fig. 3.11 2oo3 electrical diagram 55
Fig. 3.12 2oo3 multi-phase Markov model 55
Fig. 3.13 Impact of safe failures on the safety integrity represented by: (a) *PFD* for 2oo2 and (b) *PFH* for 1oo2D 58
Fig. 3.14 (a) impact of dangerous failures on *PFS* for the 1oo1 and (b) impact of the *DC* value on *STR* for the 1oo2D 62
Fig. 4.1 Markov model of a component subject to DD/DU failures and PT 66
Fig. 4.2 Markov model of a component subject to DU failures, partial and proof tests 70
Fig. 4.3 Generic approached Markov model for *K*oo*N* architectures: (a) independent safe failures and (b) dependent safe failures (CCF) 78
Fig. 4.4 Markov models for 2oo2 configuration: (a) multi-phase and (b) approximated models 81
Fig. 4.5 *PFS(t)* and *STR(t)* for 2oo2 architecture obtained from: (a) multi-phase and (b) approximated models 81
Fig. 5.1 Relationship between Belief, Plausibility and Uncertainty 90
Fig. 5.2 Frequency distribution of: (a) PFD_{avg} and (b) *PFH* 96
Fig. 5.3 Cobweb plot of PFD_{avg} and its input parameters 97
Fig. 5.4 Evidential network of the 2oo3 subsystem 98
Fig. 5.5 PFD_{avg} of the 2oo3 subsystem and its related parameters in the context of evidential networks 100
Fig. 5.6 Sensitivity analysis for PFD_{avg} and *PFH* of the 2oo3 subsystem when the inputs are given as intervals 101
Fig. 5.7 PFD_{avg} and *PFH* of the 2oo3 subsystem represented as hybrid numbers (P-boxes) 103
Fig. 5.8 Sensitivity analysis for PFD_{avg} and *PFH* of the 2oo3 subsystem when the inputs are with different natures 104
Fig. 5.9 Histograms related to PFD_{avg} and *PFH* for S, LS, FE and SIS 106
Fig. 5.10 Cumulative distribution function of PFD_{avg} and *PFH* 106
Fig. 5.11 Fuzzy numbers related to PFD_{avg} and *PFH* for S, LS, FE and SIS 107
Fig. 5.12 Possibility and necessity measures for a given SIL_{RU} 109
Fig. 5.13 Compliance probability principle 110

Fig. 5.14 Overall process for combining MC and fuzzy sets 110

Fig. 5.15 Confidence interval for the average fuzzy number 112

Fig. 5.16 Average fuzzy numbers related to PFD_{avg} and *PFH* 115

Fig. 5.17 Histograms and CDFs for COGs related to the SIS PFD_{avg} and *PFH* 115

Fig. 5.18 The SIS's PFD_{avg} and *PFH* confidence intervals 116

Abbreviations

ANOVA	Analysis of Variance
avg	Average
Bel	Belief
BFR	Binomial Failure Rate
CCCG	Common Cause Component Group
CCF	Common Cause Failure
CDF	Cumulative Distribution Function
COG	Center of Gravity
DC	Diagnostic Coverage
DD	Dangerous Detected
DST	Dempster-Shafer Theory
DU	Dangerous Undetected
E/E/PE	Electrical/Electronic/Programmable Electronic
eFAST	Extended FAST
EN	Evidential Network
ESD	Emergency Shut-Down
EUC	Equipment Under Control
FAR	Fatal Accident Rate
FAST	Fourier Amplitude Sensitivity Test
HFT	Hardware Fault Tolerance
ind	Independent
K(M)ooN	N(M)-out-of-N
LOPA	Layer of Protection Analysis
LOPC	Loss of Primary Containment
MBF	Multiple Beta Factor
MC	Monte Carlo
MDT	Mean Down Time
MGL	Multiple Greek Letter
MPM	Multi-Phase Markov
MRT	Mean Repair Time
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair (restoration)
MUT	Mean Up Time
OAT	One-At-a-Time
PBA	Probability Bounds Analysis
P-box	Probability Box
PCC	Partial Correlation Coefficient
pdf	Probability Density Function
PEAR(PPMCC)	Pearson Product-Moment Correlation Coefficient
PFD	Probability of Failure on Demand
PFH	(Average) Probability of Failure per Hour
PFS	Probability of Failing Safely
Pl	Plausibility
PRA	Probabilistic Risk Assessment (Analysis)
PRCC	Partial Rank Correlation Coefficient

PSM	Process Safety Management
PST	Partial Stroke Testing
PT	Proof Testing
PTC	Proof Test Coverage
RAMS	Reliability, Availability, Maintainability and Safety
RSS	Residual Sum of Squares
RU	Required Upper Bound
SA	Sensitivity Analysis
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SIS	Safety Instrumented Systems
SPEA	Spearman Rank Correlation Coefficient
SRC	Standardized Regression Coefficient
SRRC	Standardized Rank Regression Coefficient
STR	Spurious Trip Rate
TFR	Trinomial Failure Rate
UA	Uncertainty Analysis
UPM	Unified Partial Method

Introduction

One of the striking features of post–World War II era is the focus of most of the leaders and regimes on taking, one way or another, the economic side as the forefront of their priorities, the aspect that has an immediate impact on the internal social and political stability as well as the external relations and geopolitical dynamics that added water, food and energy security to the collection of parameters they are controlled by. Such propensity has become a necessity in the global village's period where the physical distances and boundaries are faded by dint of the informational revolution, which has mightily helped in raising people's aspirations for more comfortable living conditions and welfare. The result is a tremendous and ceaseless escalation of the demand on water, goods and energy. To exemplify, the BP Company is expecting in its energy outlook (BP, 2014) that primary energy demand increases by 41% between 2012 and 2035, with growth averaging 1.5% per annum, where industry remains the dominant source of growth for primary energy consumption, both directly and indirectly. Under these circumstances, the negative effects are not only limited to the exhaustion of the raw materials and natural resources but they also extend to the direct and immense impact of the industrial facilities, which can be described by their pivotal role in the economy's engine and their continuous growth in terms of spread, size and risk on human being (health and safety) and environment that has already reached a momentous degree of damage.

With the augmentation of its threats that never stop on showing how severe they could be, industry is obliged to prove that a certain acceptable level of risk is guaranteed. Actually, the current practice, which reflects the accumulation of tens of years of experience, emphasizes that several technical and organizational measures must be employed and distributed over several levels to prevent the occurrence of the undesired events and protect the vulnerable targets. It is well known that the automatic systems constitute an indispensable and irreplaceable element in the process of risk reduction in almost all of nowadays' industrial facilities. Taking advantage of the giant technological and practical advancements, those safety devices are witnessing a continuous development in terms of efficiency and sophistication. To a large extent, it has been recognized that a comprehensive approach must be adopted to accompany the automatic safety systems throughout their lifecycle in order to manage their criticality and complexity, the matter that is reflected by the engendered standards, codes and techniques in this context. In addition to ensuring that the safety purposes are appropriately defined, measured, carried out and pursued, the usefulness of such approach includes the avoidance of the problem of over-design whose implications are twofold: a) superfluous cost at several stages and b) higher likelihood of occurrence of the spurious shutdowns that result from the erroneous activation of the safety functions due to the so-called safe failures.

The IEC 61508 is an international functional safety-related standard that adopts an overall safety lifecycle approach as a technical framework for the coverage of all of the involved steps and functions in the process of reducing risks to a certain tolerable level that includes the intervention of the electrical / electronic / programmable electronic (E/E/PE) safety-related systems. This generic standard, which gained an important attention within the industrial and scientific communities, represents a foundation of many specific product and application sector standards like the IEC 61511 that exclusively deals with the process industry sector. However, the provided lifecycle holds multiple activities from the initial concept, though design, implementation, operation and maintenance to decommissioning of the safety instrumented systems (SISs), which correspond to the (E/E/PE) safety-related systems in the process industry sector. Those activities are habitually categorized into three distinct phases, which are the analysis, realization and operation.

Indeed, one of the key steps in the realization phase that has a forthright effect on the whole process is the quantitative evaluation of the performance of SISs to verify their ability to suitably accomplish their intended safety instrumented functions (SIFs) whose magnitudes are defined via the concept of safety integrity level (SIL). For the physical hardware portion, such evaluation is customarily probabilistic based on the estimation of the average probability of failure on demand (PFD_{avg}) and average probability of failure per hour (PFH), where each metric is dedicated to a specific demand mode of operation. However, these performance indicators are functions of a variety of types of factors and parameters, such as failure rates, testing capabilities and intervals, and repair times. Finding an appropriate formalization for those elements is the challenging task because of the involved behaviors and interactions what requires the use of several simplifications and assumptions to handle that complexity that worsens as the number of the redundant components increases. A large number of tools and techniques could be employed for the sake of reliability modeling of the performance of SISs like Reliability Block Diagrams, Fault trees, Markov models, Petri nets, etc., where the selection entails the observance of the criteria of easiness and capability to take the various characteristics into consideration.

As the SISs can cease to provide the intended function when it is required (potentially unsafe conditions), it also common that they go to the other extreme by falsely activating the safety function when there is no need for it. According to (Lundteigen, et al., 2008 (a)), such undesirable disruptions may lead to production loss, stress on affected components and systems, and hazards during system restoration. The significance of those consequences necessitates the assessment of this performance side of SISs, which is known as operational (production) integrity, during the designing stage to forecast the spurious trips' occurrence and judging their acceptance. There exists several metrics in the context of operational integrity like the average probability of failing safely (PFS_{avg}), spurious trip rate (STR) and mean time to failure-spurious ($MTTF_{spurious}$). Similarly to the safety integrity's ones, these latter performance indicators are functions of several ingredients that should be properly structured.

Indubitably, modeling the performance of SISs is quite delicate and intricate, where the occasions of mistaking are numerous and their disclosure may not be very accessible whereas even the smallest mistakes can affect the credibility of the ultimate results. In this context, it is explicitly pointed out in the sixth part of the IEC 61508 that it is very important that the user of a particular technique is competent in using the technique and this may be more important than the technique which is actually used. Under many factual circumstances, the simplified equations approach represents the best possible and safest alternative. One of the principal objectives of this thesis is to provide a new formulation for the various performance indicators of both safety and operational integrity that bridges several gaps in the already existing ones. Besides the consideration of the various involved features (e.g., CCF events and PST) the proposed formulas should be generalized to handle any *KooN* architecture and, most importantly, hold certain simplicity in implementation and flexibility in adapting them to many possible situations. Prior to that, it is important to investigate some comprised choices and hypotheses like the selection of the model to be used for the quantification of CCF events' contribution and the exclusion's impact of certain constituents.

Uncertainty is thoroughly embedded in the evaluation of the performance of SISs under several forms and types, the concern that must be understood and addressed. An in depth description and clarification of this aspect would be presented in purpose of correctly deciding on which is the treatment way that can fit the nature and specificity of SISs. Another related objective is weighing the contribution of each source to the overall uncertainty in the outputs.

This thesis consists of five chapters. Chapter 1 is entirely dedicated to the study of the various relevant terms, concepts and notions in purpose of clarifying the relationships between them and attempting to demystify some of the prevalent confusions in such scope. The aim of chapter 2 is to scrutinize the CCFs that have the leading role in most of the situations with an utter focus on the different models that could be used to quantify the contribution such events. The effect of neglecting the safe failures in the evaluation of the safety integrity on the one hand and the dangerous failures in the evaluation of the operational integrity on the other one is the theme of chapter 3. Chapter 4 is devoted to modeling the performance of SISs by proposing new generalized formulas for all of PFD_{avg}, PFH, PFS_{avg} and STR, while the analysis of both uncertainty and sensitivity is the content of chapter 5.

1. BASIC CONCEPTS' CLARIFICATION

It is recognizable that even the simplest activities in the everyday life are accompanied by certain relative risks, the fact that necessitates the human being to learn how to deal with their existence since a very young age. Not to mention the industrial activities which mainly rely on extremely complex and sophisticated technologies and usually highly hazardous substances. In brief, an industrial *hazard* is defined in (IAPA, 2007) as "*The potential of any machine, equipment, process, material (including biological and chemical) or physical factor that may cause harm to people, or damage to property or the environment*", while the concept of *risk* is considered in (Crowl, et al., 2011) as "*a measure of human injury, environmental damage, or economic loss in terms of both the incident likelihood and the magnitude of the loss or injury*". Actually, any effort to reduce the incident likelihood is viewed as a *prevention* measure, whereas working on the magnitude of the consequences is customarily considered as a measure of *protection* or *mitigation*.

Over the years, the industrial community has developed several approaches, means and techniques in purpose of facing up to such events. The unfortunate industrial accidents that occurred all over the world have contributed in revealing many gaps in the way the industrial safety is regarded and dealt, and also helped to the dissemination of the public awareness concerning this issue, the fact that added an extra pressure to ensure a certain level of safety that goes along with the complexity and riskiness of the dealing with systems and materials. Today, the industrial safety has reached an important and compound level, the truth that can be verified through the advanced management strategies, the abundance of the related tools and data, and also through the effectiveness and accuracy of the technical safeguarding measures.

This first chapter is utterly devoted to provide a theoretical summing up of the current practice and perception regarding the concept of safety, its relationship with many other close concepts and theories as well as its partitions and the means it relies on to attain that major goal. Indeed, among those means the highlight will be focused on the *safety instrumented systems* (SIS) and their corresponding notions and standards, since they are the hub of this work and such description is indispensable for the rest of chapters.

1.1 Dependability

The early years of the twentieth century witnessed an unprecedented growth in terms of systems' technology used in the different fields of industry. That growth at that point was a logical continuation to the previous century's innovations such as battery, automobile, electricity,… and a necessity to keep up first with the political, economic and social instability (world wars, great depression, etc.) of that period and then with the insatiable productivity which was supplied by the immense rising demand for more goods and services with certain level of quality which, in turn, reflected the evolution in the standards of living in several parts of the world. To deal with the fact that the systems become more complex and the traditional practice become unable to cope with that situation, new disciplines have appeared progressively such as *control engineering, logistics engineering, reliability engineering, performance engineering*,… to manage that complexity. Later on, those disciplines have been gathered under the name of *system engineering*. Within this latter the concept of *dependability* has came into view, which is considered at the beginning as a synonym of reliability but it soon took its appropriate track.

In fact, there is no consensus on how to define dependability or what it should comprise. It is a broad concept and it has a considerable flexibility that allows it to take different forms and handle different notions. In what follows we cite some of the widely accepted definitions in purpose of taking a quick look at the meaning of dependability from different corners.

Starting first by (Villemeur, 1988), in which dependability is considered as: a) the science of failures that includes their knowledge, evaluation, prediction, measurement and mastery, and more strictly b) the ability of an entity to satisfy one or more required functions under given conditions. In a similar fashion, (Avizienis, et al., 1986) considers dependability as a property of a computer system that allows reliance to be justifiably placed on the service it delivers. Later on, the providers of this latter definition have amended it in purpose of making it more convenient and in line with the definitions of its attributes, where it is defined in (Avizienis, et al., 2000) as the ability to deliver service that can justifiably be trusted.

The standard (EN 13306, 2010) defines dependability as the ability to perform as and when required. Moreover, the characteristics of this latter include availability and its inherent or external influencing factors, such as: reliability, fault-tolerance, recoverability, integrity, security, maintainability, durability and maintenance support. The upcoming elucidation of the different attributes of dependability will show that this definition is somehow abridging this latter in one of its constituents, which is the availability concept.

The acronym RAMS (Reliability, Availability, Maintainability and Safety) substitutes the term dependability in many documents such as (IEC 62278, 2002). In fact, dependability is much larger because it takes into account the ingredients of this acronym and many other ones. However, from this sample of definitions, it can be concluded that dependability is an umbrella term, where its constituents may vary from an area to another.

The dependability tree (see Fig. 1.1) has been used for many years in many references such as (Avizienis, et al., 1986; Laprie, 1995 (a); Laprie, 1995 (b); Avizienis, et al., 2000) to describe the structure of dependability and how its constituents are interconnected. Actually, this tree has passed through several stages to reach this format which is obtained from (Avizienis, et al., 2004). In what follows, a brief description of the various constituents of the tree will be provided.

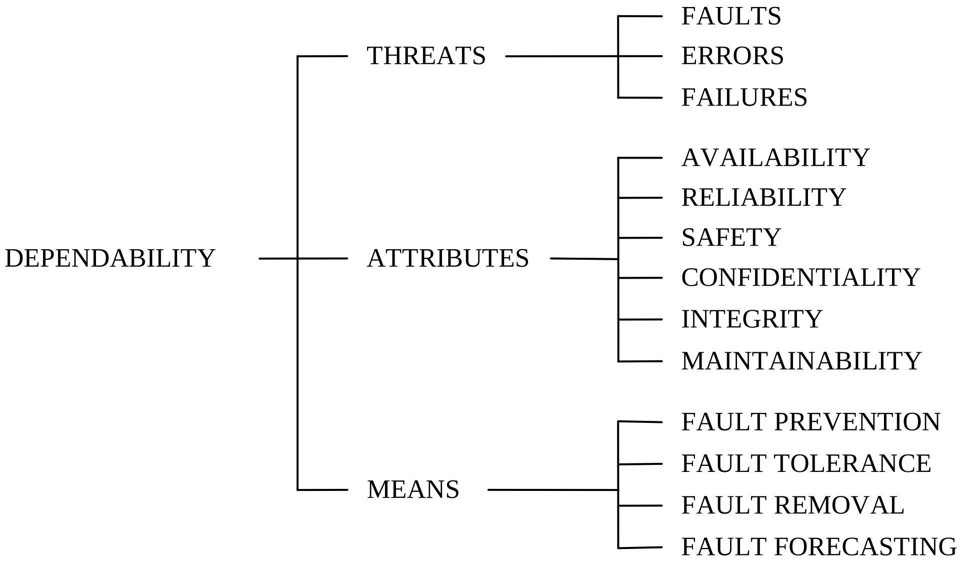


Fig. 1.1 The dependability tree (Avizienis, et al., 2004)

1.1.1 Threats

Also known as *impairments* and as it appears from the tree, they cover *faults*, *errors* and *failures*. Like their names imply, those notions can elicit unpleasant situations, disturbances or harms to the system's dependability, in other words, they are able to prevent the system (or part of it) from properly fulfill its function.

- **Faults:** could happen at any stage of the system's lifecycle and they denote weak, wrong or imperfect actions, circumstances or things that happen inside the system itself or in its environment, where their consequences may be limited to this extent or upgrade to more serious levels.
- **Errors:** basically follow faults, they may be detectable or not. In fact, they represent the inconsistency between the desired and the existent performance of the system. Under some conditions they can generate other errors or even lead to the failure of the system.
- **Failures:** simply defined by the Oxford dictionary as *the actions or states of not functioning*. A failed system represents any system with no ability to fulfill its planned function. They are typically caused by errors. Furthermore, the manner in which a system fails is called *failure mode*.

It should be noted that there is no accord on which one of the three concepts occur before the other, and contrary to what it has been stated here many consider that faults result from failures. Also many consider that the main difference between a fault and a failure lies in the fact that the first is a state where the other is an event. In this context, (Cheol Kim, et al., 2015) reviews many definitions related to those terms.

1.1.2 Attributes

The dependability's attributes stand for a set of metrics that essentially aim to gauge its performance, like the readiness and/or the continuance of delivering a correct service. As it has been mentioned earlier, other than those metrics listed in the tree and will be targeted hereinafter, many other ones can be found that depends on the scope and the user's need.

In point of fact, before introducing those attributes, it would be quite useful to pass through certain essential concepts. Let the random variable $T \geq 0$ to be the time to failure of a given item, with a certain distribution (e.g., exponential, weibull, gamma and normal). Then, $F(t)$ is the *cumulative distribution function* (CDF) of this latter, which represents the probability that the corresponding item will fail in the interval [0,t], and $f(t)$ is its *probability density function* (pdf) that is defined in Eq. (1.1).

$$f(t) = \frac{dF(t)}{dt} = \lim_{\Delta t \to 0} \frac{Pr(t < T \leq t + \Delta t)}{\Delta t} \tag{1.1}$$

The term $f(t)\Delta t$ symbolizes the (unconditional) probability that the item will fail in the time interval ($t, t+\Delta t$]. In fact, it is more popular and useful within the dependability studies to employ the conditional probability that the item will fail in the time interval ($t, t+\Delta t$] given that this latter item has remained immune to failures until the time t. This conditional probability is customarily denoted by $\lambda(t)\Delta t$ and extracted from the next equation:

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{Pr(t < T \leq t + \Delta t | T > t)}{\Delta t} = \frac{f(t)}{1 - F(t)} \tag{1.2}$$

The function $\lambda(t)$ is known as *failure rate function* or *hazard rate function* and it forms one of the most significant concepts in the field of dependability. Obviously, it can be interpreted as the probability of failure in an infinitesimal unit interval of time (Finkelstein, 2008). It is common to assimilate the form of the failure rate function over the item's lifetime (especially the electronic ones) to the bathtub curve (see Fig. 1.2).

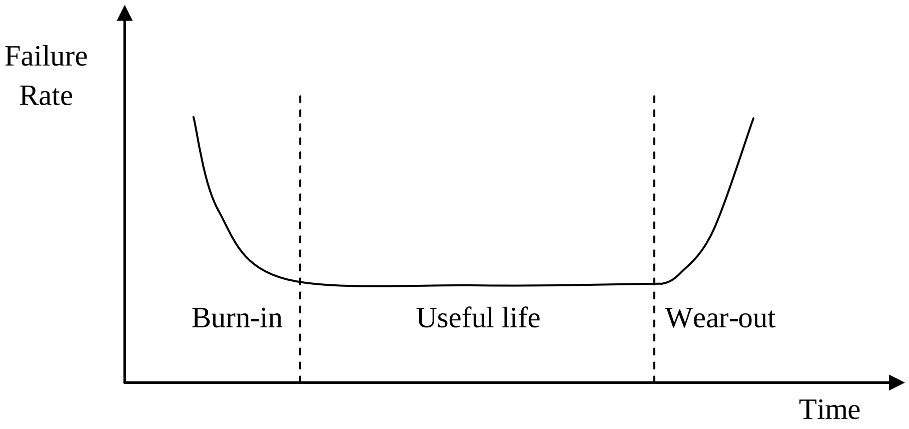


Fig. 1.2 Bathtub curve

Three distinct regions (or phases) can be noticed in the bathtub curve. The *burn-in* region represents the early life of the item where the failure rate begins high and then decreases until it reaches the *useful life* phase, in which the failure rate remains almost constant, particularly for the electronic items. Lastly, in the *wear-out* phase the failure rate increases as the functioning time is running. Table 1.1 provides some of the failures' causes in each phase.

Table 1.1 Reasons of the occurrence of failures in the three regions of the bathtub curve (Dhillon, 2006)

Phase	**Cause**
Burn-in	Poor manufacturing methods Poor process Poor quality control Poor debugging Human error Substandard materials and workmanship
Useful life	Low safety factors Undetectable defects Human errors Abuse Higher random stress than expected Natural failures
Wear-out	Wear-out caused by friction Poor maintenance Incorrect overhaul practices Corrosion and creep Short designed-in life of the item Wear caused by aging

In fact, other useful concepts are extensively used in this field, namely: *MTTF*, *MDT*, *MUT* and *MTBF*. Actually, Fig. 1.3 that is obtained from (Villemeur, 1988) provides one of preeminent ways to explain the relationship between these different notions.

- ✓ *Mean Time To Failure (MTTF)*: represents the expected value of *T*, it is useful for the non-repairable items. Mathematically, *MTTF* can be defined as follows:

$$MTTF = \int_{0}^{\infty} tf(t)dt \tag{1.3}$$

- ✓ *Mean Down Time (MDT)*: is the expectation of the total down time, it includes the needed time to detect and repair the failure as well as the needed time to return the item into service. In other words, the well known *Mean Time To Repair (MTTR)* belongs to the *MDT*, and it can substitute it whenever the other two related times considered relatively less important.
- ✓ *Mean Up Time (MUT)*: after the occurrence of the failure, detecting and repairing it, *MUT* represent the expected time between the moment of returning the item to perform its intended function till the occurrence of the next failure. Conversely to *MTTF*, *MUT* is the utilized one for the repairable items.
- ✓ *Mean Time Between Failures (MTBF)*: is the expected time between two consecutive failures. *MTBF* can be expressed in terms of *MDT* and *MUT* as follows:

$$MTBF = MDT + MUT \tag{1.4}$$

It should be noted that in many cases the term *MTBF* is used instead of *MUT*, this fact can be referred whether to the unpopularity of this latter or the negligence of *MDT* compared to *MUT*.

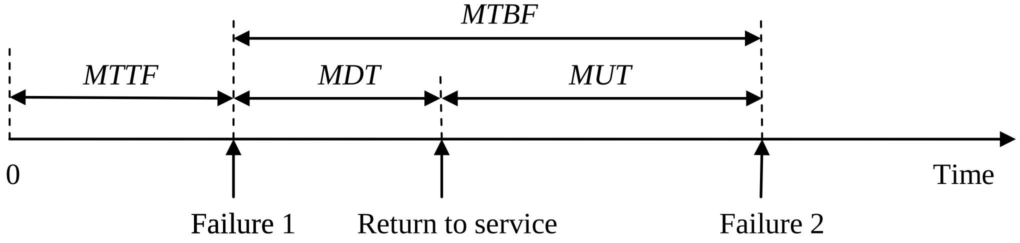


Fig. 1.3 Representation of *MTTF*, *MDT*, *MUT* and *MTBF* (Villemeur, 1988)

- **Availability**

This attribute is related to the repairable systems, it is defined in (IEC 60050, 1999) as the ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the external resources are provided. Regardless how many times the corresponding item has failed and repaired formerly, its availability represents its readiness of correctly functioning. Actually, the reader should be aware that there exist several meanings and interpretations of availability, while some of them are used more frequently than others. The three most famous kinds of availability are the *instantaneous availability*, *average availability*, and *steady state availability*:

- ✓ *Instantaneous (point) availability*: as its name indicates, the instantaneous availability focuses on the ability of suitably performing at the specific instant *t*. It can be written in the following manner (Shooman, 2002):

$$A(t) = \Pr(no\ \ failure\ in\ [0,t] + 1\ \ failure\ and\ 1\ repair\ in\ [0,t] + \cdots) \tag{1.5}$$

- ✓ *Average availability*: aka, *interval availability* represents the average of the former availability over a given period of time *Z*.

$$A_{avg} = \frac{1}{Z}\int_{0}^{Z} A(t)dt \tag{1.6}$$

- ✓ *Steady state availability*: usually deemed as *asymptotic availability* or *limit availability*, which represents the limit of the instantaneous availability as time tends to infinity:

$$A(\infty) = \lim_{t\to\infty} A(t) \tag{1.7}$$

Also, it is habitually computed as follows:

$$A = \frac{MUT}{MDT + MUT} \tag{1.8}$$

- **Reliability**

As an attribute, reliability is habitually defined as the ability of an item to perform its required function under given conditions for a certain time interval [*0*, *t*], given that it was functioning properly at *t=0*. From a quantitative viewpoint, that ability is simply handled as probability and denoted by *R(t)*.

$$R(t) = Pr(T > t) = 1 - Pr(T \le t) = 1 - F(t) \tag{1.9}$$

Where, *F(t)* is the *unreliability,* which is in fact, the CDF of *T*.

- **Safety**

Sharing the use of the same tools and methods had created a sort of confusion between safety and other traditional attributes (reliability in particular), but the outcrop of many terms such as safe/unsafe failures has put an end to that bafflement. Safety could be viewed as: a) the freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment (MIL-STD-882D, 2000), or merely as b) the ability of an item to keep all over its lifecycle an acceptable level of risk that could constitute a threat of any kind to human being, good, and/or environment.

- **Confidentiality**

Irrefutably, data and information are a priceless treasure that must be tightly protected and kept away from the not permitted individuals' access. According to (Rogers, et al., 2009), confidentiality is violated whenever sensitive or proprietary information is disclosed to any unauthorized entity (human, program, or computer system). Encryption is commonly renowned as a powerful tool to boost confidentiality.

- **Integrity**

Actually, this attribute is somewhat interrelated with the preceding one. It is defined in (Avizienis, et al., 2004) as the absence of improper system alterations. In reality, the seriousness of this attribute lies in its capability to directly impinge on the other ones. In other words, the infringement of this latter can be overwhelming for other attributes like safety, reliability and/or availability since the relied upon information became fallacious.

- **Maintainability**

To end with maintainability, which is defined in (MIL-STD-721C, 1981) as the measure of the ability of an item to be retained in or restored to specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair. The beforehand seen *MTTR* is the basic measure of this fundamental dependability's attribute.

To seal this topic, let us mention the confidentiality, integrity and availability form jointly one of the core features of *security,* which is well known as the *CIA triad*.

1.1.3 Means

Opposing the threats, means of dependability represent a set of tools, measures or defensive barriers that endeavor to enhance the system's dependability, by confronting those previously discussed threats. They are habitually split into four categories, where they cover the entire lifecycle of the system.

- **Fault prevention:** by acting early (i.e., eliminating all the possible causes that have the potential to generate faults), this practice is intended to keep the item away from faults and therefore errors and failures.
- **Fault tolerance:** is an important and widely used technique to guarantee the continuation of the function, even with the existence of certain number of faults and errors. Indeed, the concept of redundancy (hardware, software, information or time) has a vital role in achieving this task.

- **Fault removal:** now, if the faults already exist, this technique typically aims to detect that existence and fix them using a combination of several procedures such as verification (which in turn employs lots of techniques like the various testing and inspection policies), diagnosis and correction.
- **Fault forecasting:** is a whole approach that seeks to process those threats in detail by predict, assess and control their occurrence. This could be done via different tools and methods such as block diagrams, Fault trees, Markov models, Petri nets, etc.

Unfortunately, the practical implementation of these means is not always trouble-free as it seems theoretically and their effects are not utterly positive. Moreover, they may contribute in increasing the complexity and therefore the undependability of the system.

1.2 Process safety

The early years of the twentieth century has witnessed the lucid birth of the concept of safety in the industrial world. That birth was not a luxury or a coincidence, but an outcome of the terrible rates of work-related fatalities, illnesses and injuries that reached deplorable levels because of the human obsession with rapid profits that escalated with the emergence of the industrial revolution. Through the effective striving of several scientists, activists and unions like Alice Hamilton, Irving Selikoff and Frances Perkins in the U.S. and in the advanced countries in general a considerable attention has been paid to this issue and the result was the drawing up of more rigorous laws, regulations and standards in order of making the workplaces safer and protecting the rights of workers concerning this matter. A tangible progress has been achieved thanks to those endeavors, the fact that can quantitatively verified through the important decline in the total number of occupational incidents. For instance, Fig. 1.4 shows the fatalities' rates in the U.S. coal mining since 1900, where the tremendous progress is observable.

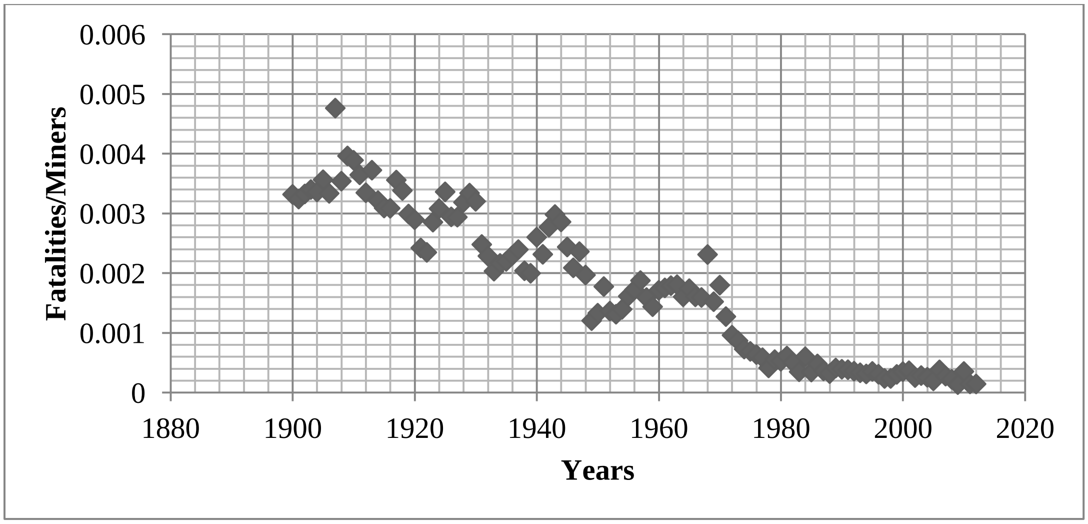


Fig. 1.4 U.S. coal mining fatalities, according to (MSHA , 2013)

Gradually, that trend of protecting the workers from the work-related hazards and risks has become a priority in most parts of the world and it is well-known today under the name of *occupational safety*. Furthermore, scientist and engineers have created over the years several metrics and indicators to measure the industrials' performance regarding that vital aspect. For example, it is advised to employ the following formula in order to compute the *Fatal Accident Rate* (FAR) that is taken for 1000 employees working for 100,000 hours during their lifetime (see (Crowl, et al., 2011) for further reading):

$$FAR = \frac{Number\ of\ \ fatalities \times 10^{8}}{\begin{array}{c} Total\ hours\ worked\ by\ all\ employees \\ during\ period\ covered \end{array}} \tag{1.10}$$

After the end of the Second World War (1939-1945) with its colossal consequences that massively affected the economic situation and exhausted the human being throughout the globe, an unprecedented gluttony towards more goods with high qualities has appeared. The bulk of the mission of dealing with that situation has entrusted to the different sectors of industry, which in turn have carried it out to the fullest. Indeed, the upshot of that important recovery and shift from a situation to another superior one was a big demographic growth, which soared from about 1.6 billion in 1901 to 6.1 billion at the end of that century. Eventually, the causal relationship between the economic conditions and the population size has created a sort of snowball where the growth of the first causes the growth of the second and vice versa.

Logically, in purpose of convoying that growth, it is required from the different sectors of industry, especially the process ones (e.g., oil and gas, chemical, food, textiles, etc.), to produce quantitatively and qualitatively, which does not mean nothing else than more industrial facilities that employs extremely complex procedures and technologies with huge amounts of highly hazardous materials and substances.

The unfortunate result of the combination of all those factors was the tragic manifestation of the so-called *major accidents* that have rocked and still rocking everywhere and causing disastrous consequences especially to persons and environment. Certainly, the horrific number of those regrettable events makes the task of exhaustively counting them in this manuscript so intricate, instead some of the most famous and change prompters ones will be briefly pointed out hereinafter. Further details can be found in the third volume of (Mannan, 2005).

- **Flixborough, England (1974)**

A ruptured bypass system at a chemical plant led to the leak of the hazardous *cyclohexane*, forming a colossal flammable vapor cloud. In contact with a source of ignition, this latter has exploded leaving more than 28 workers killed and 36 injured in addition to the complete destruction of the entire plant. This accident has led to the set up of the Advisory Committee on Major Hazards.

- **Seveso, Italy (1976)**

A dense white vapor cloud of *TCDD* (type of dioxin witch known as a carcinogenic and extremely poisonous substance) released through the relief valve of a reactor in a chemical plant manufacturing pesticides and herbicides causing the contamination of approximately ten square miles of land, the matter that led to the evacuation of more than 600 habitants and treating 2000 people for dioxin poisoning in addition to the important fauna and flora losses. This disaster was the primary cause to adopt the so-called *Seveso Directives* throughout the European continent.

- **Bhopal, India (1984)**

More than 43 tons of the poisonous *methyl-isocyanate* (MIC) gas escaped into the atmosphere from a pesticide plant in exposure of 500,000 persons living around the factory. About 8,000 innocent were killed during the first days and almost 100,000 significantly injured. Incontrovertibly, the huge number of deaths and how dreadfully they have been killed in addition to the long term effects (e.g., cancers and deformities) make this accident the worst industrial disaster in history.

- **Mexico City, Mexico (1984)**

A series of BLEVE (Boiling Liquid Expanding Vapor Explosion) explosions in the form of domino effect initiated by an UVCE (Unconfined Vapor Cloud Explosion) took place at a LPG (Liquefied Petroleum Gas) terminal. In addition to the entire facility, a large part of the local town of *San Juan Ixhuatepec* has been devastated. The human tolls were estimated by 500 fatalities and around 5000 people severely injured.

As it has been mentioned earlier, those four major accidents are a little sample of many other ones such as Pasadena (1989), AZF Toulouse (2001) and Venezuela (2012). Locally, in 2004 an explosion rocked one of the world's biggest LNG (Liquefied Natural Gas) plants located in Skikda, destroying three of the six liquefaction trains and leaving 27 people dead and 74 others injured. This catastrophic event has attracted a big national attention to the vital role of industrial safety and the result was more stringent and control on the application and use of the *safety reports* through several laws and decrees like (JORA, 2004; JORA, 2006; JORA, 2007).

In purpose of coping with that emerging threat, a new branch of safety has come into view which principally focuses on minimizing the occurrence likelihood and cruelty of such major accidents. Within the process industries that branch became known as *process safety* and in some references *loss prevention*. Process safety is defined in (API) as a disciplined framework for managing the integrity of hazardous operating systems and process by applying good design principles, engineering, and operating and maintenance practices. Indeed, there is a vast difference between the occupational safety and the process one. As illustrates the following figure, the occupational safety related events (e.g., falls and electrifications) are frequent and relatively less severe since they affect a limited number of employees, while the process ones (e.g., fires and explosions) are rare but have very tough impacts not only on the corresponding facility zone but on its human and natural environment as well.

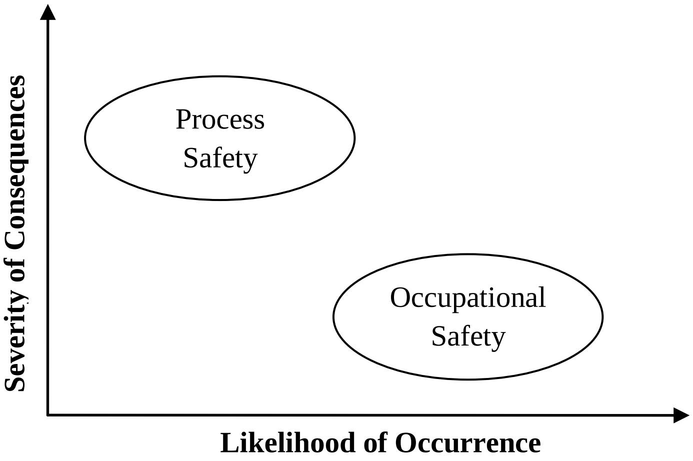


Fig. 1.5 Occupational safety vs. process safety

Several regulations and standards have been enacted in order of organizing the facilities that include major-accident hazards and ensuring that the generated risks are deeply defined, analyzed and controlled. After the Seveso disaster, the member states of the European Union adopted in 1982 the Council Directive 82/501/EEC on the major-accident hazards of certain industrial activities (Seveso I) (OJ, 1982) that was replaced later by the Council Directive 96/82/EC on the control of major-accident hazards (Seveso II) (OJEC, 1997) in 1996 and lately by the Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances (Seveso III) (OJEU, 2012). Those replacements and many other modifications, emendations and extensions reflect principally the learned lessons from the occurrence of major tragedies in different parts of the world. However, the gist of Seveso directives is the so-called *safety report*, which should be prepared by the operator of the *upper-tier* establishments and under his responsibility. According to (OJEU, 2012), the following five elements represent the outlines of the minimum data and information to be considered in the safety report. Yet, many documents like (INERIS – DRA, 2006) can be very helpful in terms of clarification and carrying out such a task.

- ✓ Information on the management system and on the organization of the establishment with a view to major-accident prevention
- ✓ Presentation of the environment of the establishment
- ✓ Description of the installation
- ✓ Identification and accidental risks analysis and prevention methods
- ✓ Measures of protection and intervention to limit the consequences of a major accident

Outside the European Union, the U.S. Occupational Safety and Health Administration (OSHA) has issued the Process Safety Management of Highly Hazardous Chemicals standard (29 CFR1910.119, 1992) that contains requirements for preventing or minimizing the consequences of catastrophic releases of toxic, reactive, flammable, or explosive chemicals, by means of the so-called *Process Safety Management* (PSM). This latter concept, which by the way is currently used in many other countries like Canada, is defined in (CCPS, 1992) as the application of management principles to the identification, understanding, and control of process hazards to prevent process-related injuries and incidents. In other words, the main objective of the PSM is ensuring that the hazardous chemicals are kept inside their equipments. The subsequent table summarizes the elements of the PSM that slightly varies from one source to another.

Table 1.2 Comparison of PSM systems (Bridges, 1994)

OSHA 29 CFR 1910.119	American Petroleum Institute	AIChE Center for Chemical Process Safety	CMA Process Safety Code
Employee Participation Process Safety Information Process Hazard Analysis Operating Procedures Training Contractors Pre-startup Safety Review Mechanical Integrity Hot Work Permit Management of Change Incident Investigation Emergency Planning and Response Compliance Audits Trade Secrets	Process Safety Information Process Hazard Analysis Management of Change Operating Procedures Safe Work Practices Training Critical Equipment and Mechanical Integrity Pre-startup Safety Review Emergency Response and Control Process-Related Incident Investigation Auditing of PHM Systems	Accountability Process knowledge and documentation Project Reviews and Design Procedures Risk Management Management of Change Process Equipment Integrity Incident Investigation Training and Performance Human Factors Standards, Codes and Laws Audits and Corrective Actions Enhancement of Process Safety Knowledge	**Management Leadership** Commitment Accountability Performance Measurement Incident Investigation Information Sharing CAER Integration **Technology** Design Documentation Process Hazards Information Process Hazard Analysis Management of Change **Facilities** Siting Codes and Standards Safety Reviews Maintenance and Inspection Multiple Safeguards Emergency Management **Personnel** Job Skills Safe Work Practices Initial Training Employee Proficiency Fitness of Duty Contractors

When it comes to metrics and indicators, the process safety is weaker than the other kind of safety, the matter that can be referred to the scarcity of occurrence of its related events (as we have seen before), and therefore a scarcity in the needed data to estimate such indicators. However, an important advancement has been made in this direction especially after the two reports (Baker III, et al., 2007; CSB, 2007) that issued in light of the 2005 BP Texas City explosion (15 deaths and more than 170 injuries) and recommend to find a common way to measure the process safety performance via the *lagging* and *leading* metrics. In response to those recommendations, a new standard was established in 2010 thanks to the effective collaboration of several organizations such as the American Petroleum industry (API) and the Center for Chemical Process Safety (CCPS). The standard is titled *Process Safety Performance Indicators for the Refining and Petrochemical Industries* (ANSI / API RP-754, 2010).

According to (CCPS, 2011), the lagging metrics are a retrospective set of metrics that are based on incidents that meet the threshold of severity that should be reported as part of the industry-wide process safety metric, while the leading ones signify a forward looking set of metrics which indicate the performance of the key work processes, operating discipline, or layers of protection that prevent incidents.

The created standard is predicated on the process safety event pyramid (see Fig. 1.6) which imitates the traditional Heinrich model. Actually, it is well known that accidents usually occur due to a series of undesired and perhaps coincided events, the fact that could be exploited by performing improvements once the very first events happen, which can be seen as symptoms or precursors, in order to avoid the occurrence of more severe events.

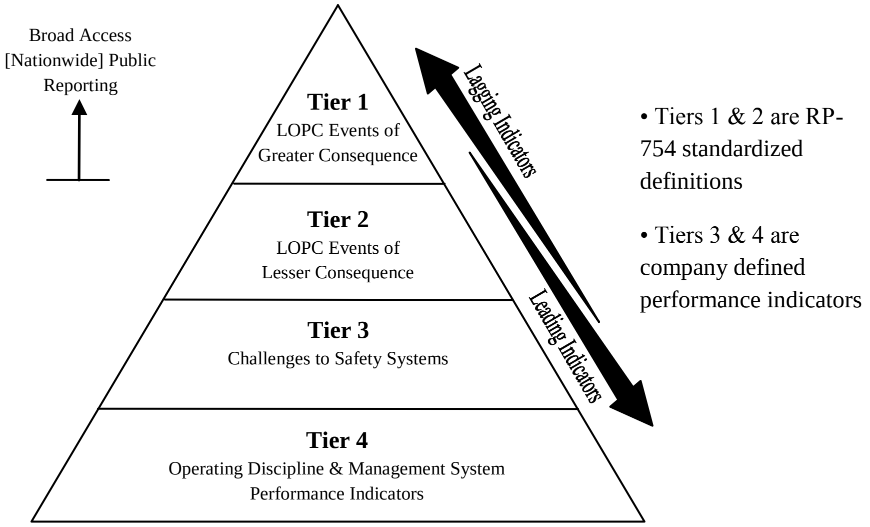

Broad Access [Nationwide] Public Reporting
Tier 1
LOPC Events of Greater Consequence
Tier 2
LOPC Events of Lesser Consequence
Tier 3
Challenges to Safety Systems
Tier 4
Operating Discipline & Management System Performance Indicators
Lagging Indicators
Leading Indicators
• Tiers 1 & 2 are RP-754 standardized definitions
• Tiers 3 & 4 are company defined performance indicators

Fig. 1.6 Process safety indicator pyramid (ANSI / API RP-754, 2010)

As depicted in the figure, the performance indicators are divided into four different tiers. Tier 1 covers the most lagging performance indicators and represents *process safety events* with greater consequences (e.g., an employee, contractor or subcontractor “days away from work” injury and/or fatality) resulting from loss of primary containment (LOPC). Tier 2 represents LOPC events with lesser consequences (e.g., an employee, contractor or subcontractor recordable injury). Tier 3 events embody challenges to the safety systems (e.g. demands on safety systems), while, the indicators of the last tier, which are the most leading represent operating discipline and management system performance.

1.3 Functional safety

Regardless the involved technology (e.g., hydraulic, pneumatic, electrical, electronic and/or programmable), the vital role of automation in the field of safety has been recognized and employed as early as such technologies became available. However, the growing complexity of the automated systems utilized for safety purposes and the criticality of such systems have necessitated the matter of framing their use and providing common practices that cover their entire lifecycle. In 1996, the International Society for Measurement and Control (ISA) issued an influential standard called Application of Safety Instrumented Systems for the Process Industries (S84.01) (ANSI/ISA-84.01-1996, 1996) that provides information related to the design and manufacture of safety instrumented systems (SIS) products, selection, application, installation, commissioning, pre-startup acceptance test, operation, maintenance, documentation and testing. Two years later, the International Electrotechnical Commission (IEC) published the famous standard "Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems" (IEC 61508) (IEC 61508, 1998) that is considered as an umbrella (generic) standard for functional safety, where it holds many sectors of industry (see Fig. 1.7).

Indeed, the emergence of such standards has contributed to the wide spreading of the "Functional Safety" concept, which is defined in the beforehand mentioned standard as "*part of the overall safety relating to the EUC*[1] *and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures*". For the process sector that is covered by the IEC 61511 standard (Functional safety: Safety-instrumented Systems for the Process Industry Sector) (IEC 61511, 2003), the term safety instrumented systems (SIS) is used instead of safety-related system. A SIS is basically composed of sensor (s), logic solver (s), and final elements(s). However, it should be noted that in the U.S., the standard IEC 61511 was accepted by ISA as (ANSI/ISA-84.00.01-2004, 2004), replacing the 1996 standard (Summers, 2007), with some modifications. It is also important to mention that in response to the ISA's inquiry regarding the relationship between S84.01 and 29 CFR1910.119, OSHA confirmed through a letter in March 23, 2000 that the S84.01 is a national consensus standard and it considers it to be recognized and generally accepted good engineering practice for SIS that are included in the Mechanical Integrity element of PSM. This matter eliminates the formation of any confusion or ambiguity and provides a sort of flexibility in implementing such a goal and ensures that the good practice is carried out smoothly. Unfortunately, such compliance is not yet unequivocally considered in the Seveso directive.

[1] EUC refers to equipment under control which represents any equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities (IEC 61508, 2010).

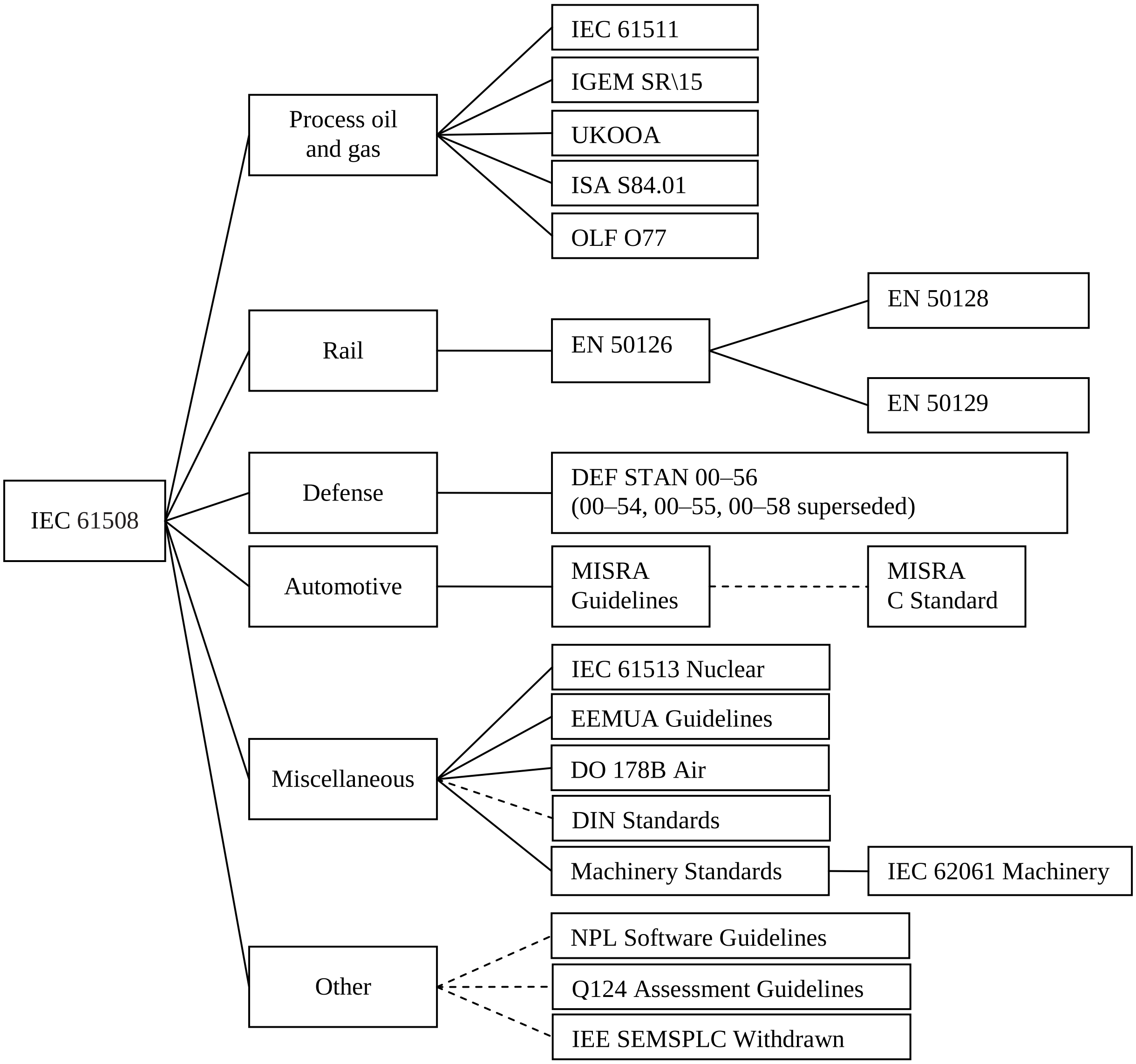


Fig. 1.7 Relationship of some standards and guidelines to IEC 61508 (Smith, et al., 2004)

Actually, most of the functional safety standards are based on the so-called *safety lifecycle*. Fig. 1.8 represents the one adopted in the IEC 61508. The main objective of a safety lifecycle is managing all the needed activities that cover all the phases (from initial concept, though design, implementation, operation and maintenance to decommissioning) of an electrical / electronic / programmable electronic (E/E/PE) safety-related systems whose failure could generates disastrous consequences on several aspects. The probability that an E/E/PE safety-related system properly carry out its intended function under all the stated conditions within a stated period of time is commonly known under the name of *safety integrity*.

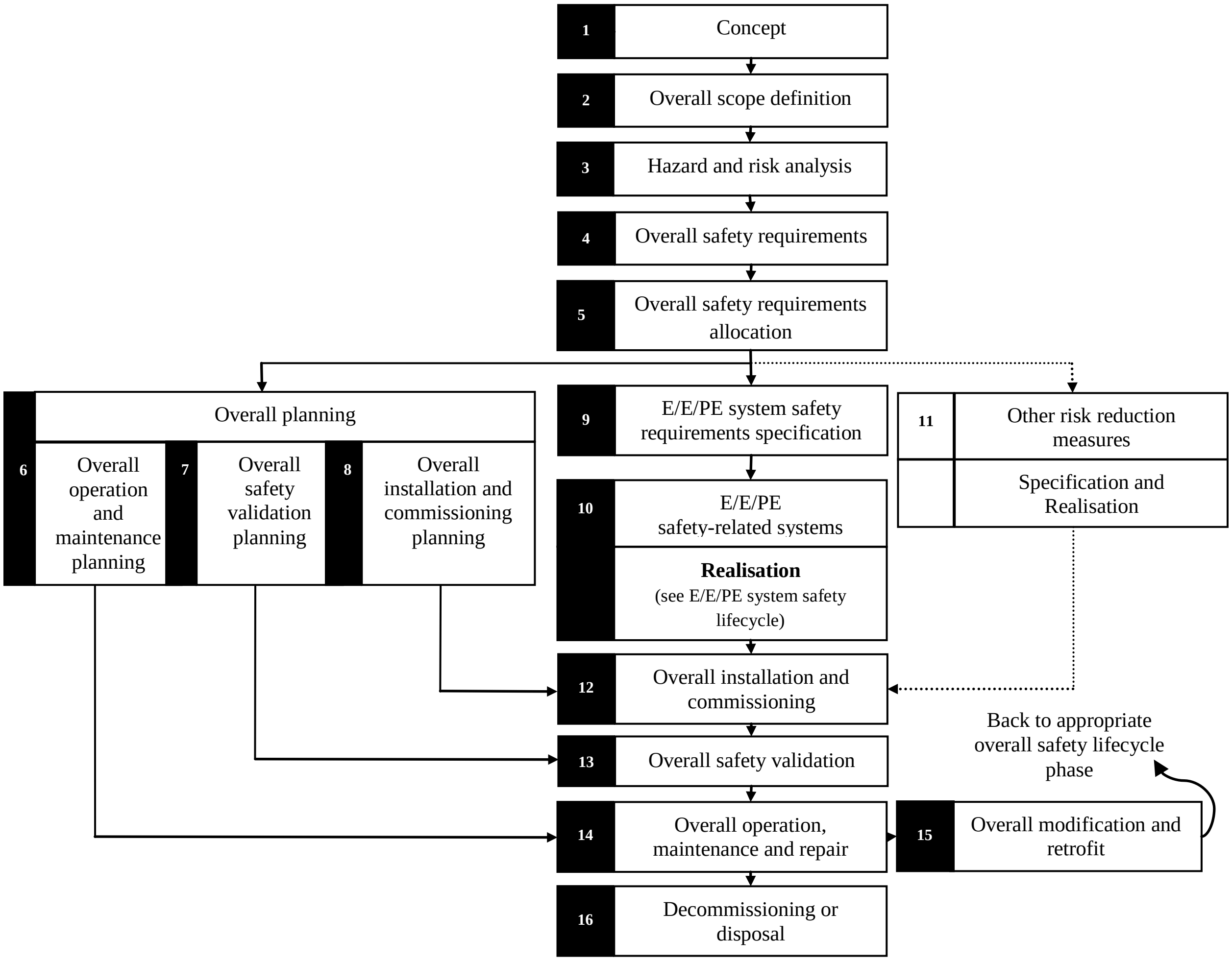

1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Overall safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 E/E/PE system safety requirements specification
10 E/E/PE safety-related systems
Realisation
(see E/E/PE system safety lifecycle)
11 Other risk reduction measures
Specification and Realisation
12 Overall installation and commissioning
13 Overall safety validation
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
Back to appropriate overall safety lifecycle phase
16 Decommissioning or disposal

Fig. 1.8 Overall safety lifecycle (IEC 61508, 2010)

It is recognized that in order to reduce the risks related to the EUC and its associated control system to a certain *tolerable* level, it is generally required to employ certain number of safeguarding measures with different technologies that intervenes in a certain predetermined manner (see Fig. 1.9). Those interventions are known as *safety functions* (e.g., process segregation, electrical isolation and deluge). Safety functions are measured using the concept of *safety integrity level* (SIL) where the SIL of a function represents the amount of risk reduction it is capable or assigned to achieve. Certainly, this concept can also be used to measure the total amount of risk to be reduced. The determination such SIL could be carried out by means of several quantitative, semi-quantitative (e.g., layer of protection analysis (LOPA)) or qualitative (e.g., risk graph method and hazardous event severity matrix) methods. Part 5 of the IEC 61508 provides a detailed description of those methods in addition to some factors that could be helpful in selecting the most suitable one.

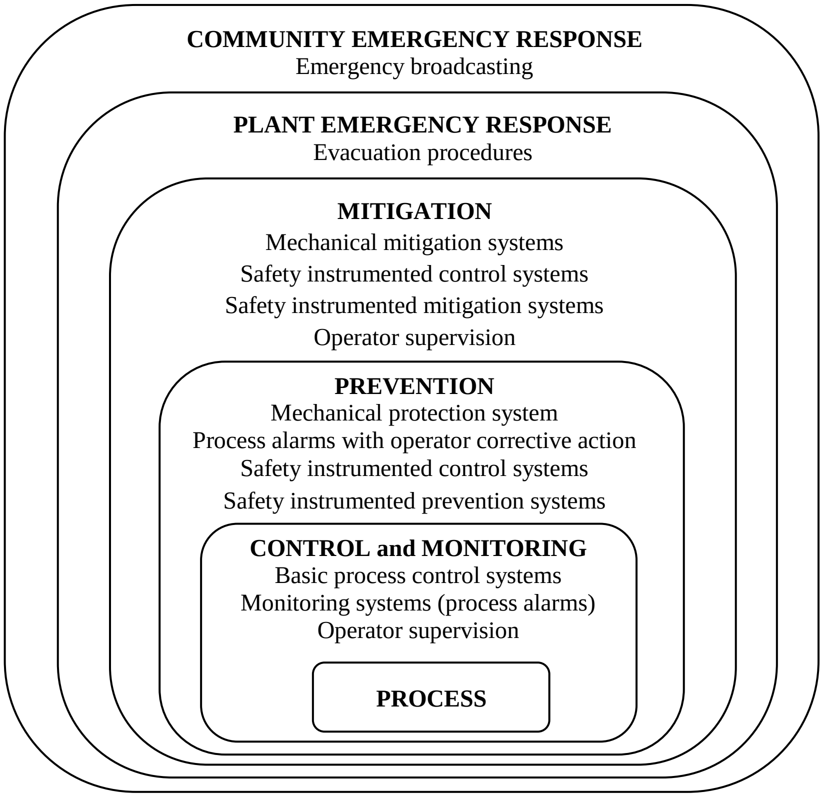

COMMUNITY EMERGENCY RESPONSE
Emergency broadcasting
PLANT EMERGENCY RESPONSE
Evacuation procedures
MITIGATION
Mechanical mitigation systems
Safety instrumented control systems
Safety instrumented mitigation systems
Operator supervision
PREVENTION
Mechanical protection system
Process alarms with operator corrective action
Safety instrumented control systems
Safety instrumented prevention systems
CONTROL and MONITORING
Basic process control systems
Monitoring systems (process alarms)
Operator supervision
PROCESS

Fig. 1.9 Typical risk reduction methods found in process plants (IEC 61511, 2003)

Obviously, the IEC 61508 is mainly concerned with E/E/PE safety related systems and it seeks through the described lifecycle to ensure that they are suitably performing their intended function. As it is mentioned in the standard, the way in which a safety function operates is called *mode of operation* that could be either:

- ✓ *Low demand mode*: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or
- ✓ *High demand mode*: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year; or
- ✓ *Continuous demand mode*: where the safety function retains the EUC in a safe state as part of normal operation.

Actually, the used criteria to distinguish between those modes of operation, which are considered ambiguous and subjective, have faced an intense criticism (see (Innal, 2008)). However, the SIL is typically split into four orders, the determination of those orders could be made using Table 1.3 for the low demand mode, where they are related to the *average probability of dangerous failure on demand* (*PFD_{avg}*) and Table 1.4 for the high and continuous demand modes, where they are given in terms of the *average probability of dangerous failure per hour* (*PFH*).

Table 1.3 Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation (IEC 61508, 2010)

Safety integrity level (SIL)	**Average probability of a dangerous failure on demand of the safety function (PFD_{avg})**
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 1.4 Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation (IEC 61508, 2010)

Safety integrity level (SIL)	**Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)**
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Depending on the manner they manifest and the consequences they yield, failures could be *dangerous,* which are able to prevent the safety function from operating when required or *safe*, which are able to cause the spurious cessation of the item's operation and therefore affect the production objectives. However, there exist two types of failures that could hit a safety-related system and cause the safety integrity's loss, namely: a) *random (physical)* failures (e.g., block of a corroded valve) and b) *systematic (functional)* failures (e.g., software crash). While the first type is usually taken into account in the estimation of the different safety integrity's performance indicators, the difficulty of quantifying and predicting the systematic failures related data has prompted the IEC 61508 and IEC 61511 to only specify some requirements that helps in reducing the occurrence of such failures. In contrast, it is suggested in (PDS, 2006) to include the contribution of systematic failures by adding a certain constant value. Furthermore, the concepts of on-line diagnostic tests and redundancy necessitate the distinction between the *detected* and *undetected* failures on the one hand, and the *dependent* and *independent* failures of the other one. On the whole, the following figure resumes the relationship between all of those kinds of failures.

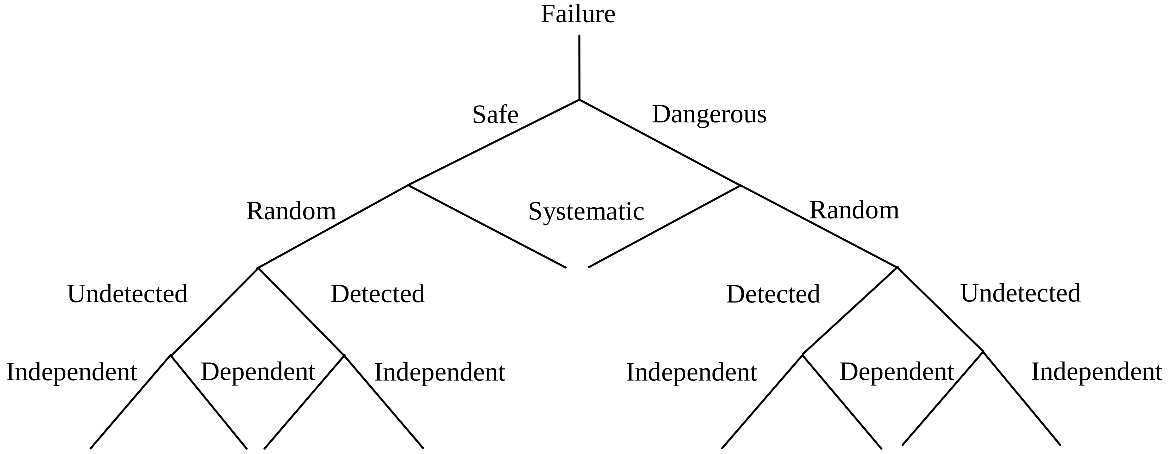


Fig. 1.10 Failures' classification

1.4 Testing policies

It is well known that improving the SIS availability and consequently the safety integrity requires the employment of several means and procedures like redundancy and tests. Redundancy is based on utilizing several channels, where each one or a group of them (depending on how they are configured (i.e., architecture)) can separately perform the required function. On the other hand, testing is very important in the direction of preceding the accident in revealing the failures' occurrence. In what follows, a brief description of the common testing policies will be targeted.

1.4.1 Automatic on-line diagnostic testing

Indeed, this type of tests has a major importance since it allows the SIS to reveal the occurrence of failures by itself in a very short amount of time. So far, three criteria are proposed in (Wolfgang, et al., 2006) that should be met in the diagnostic test, namely: a) it is carried out automatically (without human interaction) and frequently (related to the process safety time considering the hardware fault tolerance) by the system software and/or hardware; b) The test is used to find failures that can prevent the safety function from being available; and c) The system automatically acts upon the results of the test. In order of measuring the effectiveness of the diagnostic testing, it is habitual to use the so-called *diagnostic coverage* (also known as the "*coverage factor*") which is defined in (Goble, et al., 1998 (a)) as the probability that a failure will be detected given that a failure has occurred. Additionally, the following equation is widely used to determine the *DC*:

$$DC = \frac{\sum \lambda_D}{\sum \lambda} \tag{1.11}$$

where, λ_D represents the detected failure rate and λ represents the total failure rate and $\lambda = \lambda_D + \lambda_U$, where λ_U refers to the undetected failure rate. By the way, it is superior to make a distinction between the *DC* for safe failures from the one for dangerous failures. Moreover, the direct estimation of the *DC* could be achieved using the Failure Mode and Effect Analysis (FMEA) method (Goble, et al., 1998 (a); Barner, et al., 2010).

1.4.2 Proof testing

The (IEC 61508, 2010) defines the proof test as a periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an "as new" condition or as close as practical to this condition. Since the proof test usually requires the shutdown of the whole system, there is a big concern to find a middle ground between making this tests as rare as possible on the one hand and ensure a certain level of SIS's availability on the other one.

From a theoretical viewpoint and as the beforehand seen definition verifies, proof tests should disclose the occurrence of all the failures and by repairing them suitably the SIS would turn out to be "as good as new". Unluckily, many factors that can be attributed to procedural, human and/or technical reasons make this concept almost unreachable especially for the non-electronic devices (see (Tiezema, 2003)). This latter fact led to the birth of the so called *imperfect testing* concept. Whereas, the simplest manner to measure that imperfectness is implementing the *proof test coverage* (PTC) concept that is defined in Eq. (1.12), other remarkable contributions like (Baradits, et al., 2009) have been made in purpose of treating this issue differently.

$$PTC = \frac{\lambda_U^{PT}}{\lambda_U} \tag{1.12}$$

where, λ_U^{PT} designates the undetected failures that could be revealed during the proof tests.

As a last point, it remains to state that the term "*functional test"* (during the operational phase) is sometimes used in parallel with the term "proof test" and in other cases (which it seems more accurate) it is given to describe the concept of testing the functionality of a hole system without really focusing on the situation of its components (redundancy) which is not the case in the proof tests where each single component should be taken into consideration.

1.4.3 Partial stroke testing

A study performed by the Offshore Reliability Data (OREDA) shows that the final elements' failures contribute to around the half of the overall SIS's failures (see Fig. 1.11), this truth creates the need to test them frequently in purpose of detect the failures as early as possible. Unfortunately, the off-line character associated with the proof tests makes the matter of performing them frequently out of the question. An on-line way of testing the final elements and more specifically the block valves has been developed that is based on bypassing the relevant valve during the test. Although, the off-line problem can be conquered using this latter technique, the cost is twofold: a) the safety function is disabled during the test, i.e. any demand of the safety function will lead directly to the accident and b) more equipments and efforts are needed to carry out such a test and even worse more human mistakes and therefore more hazards are associated with the process of bypassing itself. The other alternative to execute an on-line test in order to identify some failure modes of a block valve without the drawbacks of the bypassing one is known as the *partial stroke testing* (PST) that relies on partially moving the valve and return it to the initial state in purpose of making sure that it is able to take the system to the safe state when it is required. The amount of moving the valve should satisfy the intended objective of the PST and in the same time ensure the continuation of the process operation. Admittedly, the usefulness of the PST has made it the focus of many papers such as (Summers, 2006; Borcsok, et al., 2007; Lundteigen, et al., 2008 (b); Brissaud, et al., 2012; Jin, et al., 2014). Furthermore, the International Society of Automation (ISA) has provided the technical report (ANSI/ISA-TR96.05.01, 2008), which addresses the applications when partial stroke testing may be useful, i.e. a decision flowchart to assist users in identification of block valves as candidates for PST and the different methods and technologies implemented in PST (mechanical limiting, position control, simplex,…).

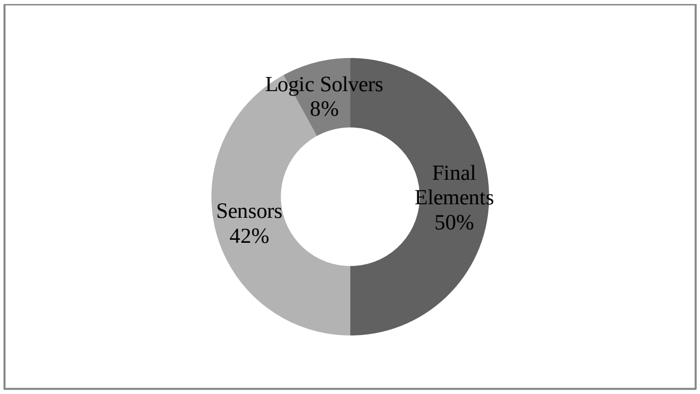


Fig. 1.11: Safety loop failures sources

The most common and easiest way of quantifying the efficiency of this type of tests in detecting failures is similar to the preceding two ones, i.e. using the fraction of the undetected failures which can be detected via the PST:

$$\theta = \frac{\lambda_U^{ST}}{\lambda_U} \tag{1.13}$$

where, λ_U^{ST} is the rate of undetected failures that can be revealed by the PSTs.

1.5 Conclusion

Evidently, the role of safety instrumented systems as a line of defense in keeping the nowadays' systems and processes safe and thus protecting all that is exposed to their hazards is very important and most of the time cannot be compensated. The other evident matter is that such safety systems are exceedingly complex and they require a particular handling throughout their lifecycle (i.e., design, implementation, operation, testing, maintenance, etc), that is why the different functional safety standards have been created and attracted such a big attention and interest.

In order to ensure that a given SIS is capable to perform its intended safety function in an approved manner it became habitual to estimate its PFD_{avg} if it functions in a low demand mode and its PFH for the high and continuous demand modes, the task that could be achieved through the employment of the various reliability tools like Reliability Block Diagrams, Fault trees and Markov models. These beforehand mentioned performance indicators are actually two functions of many factors such as architecture, dangerous failure rate, repair rate, common cause failures (CCFs) as well as the contribution of the different testing policies.

It should be noted that in the following chapters all the failure and repair rates are considered constant, in other words, time to failure and time to repair which are two random variables as we have seen in the first section of this chapter, are assumed to be exponentially distributed. What is more, many assumptions and choices should be made during the process of modeling the SIS behavior, while the consensus about the accurate alternative is usually absent. For instance, several models are available to weigh up the contribution of CCFs, whilst engineers prefer the simplest one that is reputed in the same time as the most conservative alternative. Additionally, it is common to assume that safe failures have no impact on the safety integrity and also the failure of the diagnostic devices is routinely disregarded. The following two chapters are dedicated to deeply investigate such confusing subjects.

2. QUANTIFICATION OF THE COMMON CAUSE FAILURES' CONTRIBUTION

The eternal battle against risks and hazardous events urged the engineers and designers within the different sectors of industry to build more sophisticated safeguard measures. The concept of redundancy has been widely recognized as an important technique to enhance the performance of those systems and therefore to reduce the risks to a tolerable level. Unfortunately, a special type of undesired events jeopardizes the functioning of the redundant systems and therefore comes to be the biggest limitation to that essential technique. Those events are known as *common cause failures* (CCFs) and form with the *cascading failures* the so-called *dependent failures*. In probability theory, two events *A* and *B* are considered dependent if:

$$P(A \cap B) = \begin{cases} P(A)P(B/A) \\ P(B)P(A/B) \end{cases} \neq P(A)P(B) \tag{2.1}$$

In fact, during the past four decades, CCF events have been largely studied, especially in the nuclear field which is considered and without doubt as the most advanced in this matter that clearly appears in terms of defense approaches, models and databases. Nevertheless, the importance of this kind of events necessitated their inclusion in the reliability and safety studies within all the sectors of industry which requires a certain level of equipments' performance.

As a result of the immense focus on this topic, the concept of CCFs has taken many forms and definitions over the years. On the whole, the IEC 61508 (IEC 61508, 2010) defines a CCF as a "*failure that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure*". (NUREG/CR-4780, 1988), which is considered as one of the earliest and it still one of the most used documents in terms of common cause event analysis, proposes three concepts to understand CCFs and dependent failures in general (see Fig. 2.1). The first concept represents a special kind of events that occur at some distinct but possibly unknown point in time, it is known as *root cause*. The second concept is the *coupling mechanism*, which is a way to explain how a root cause propagates to involve multiple equipment items. The last concept and according to the same document represents the existence or lack of engineered or operational defenses against unanticipated equipment failures.

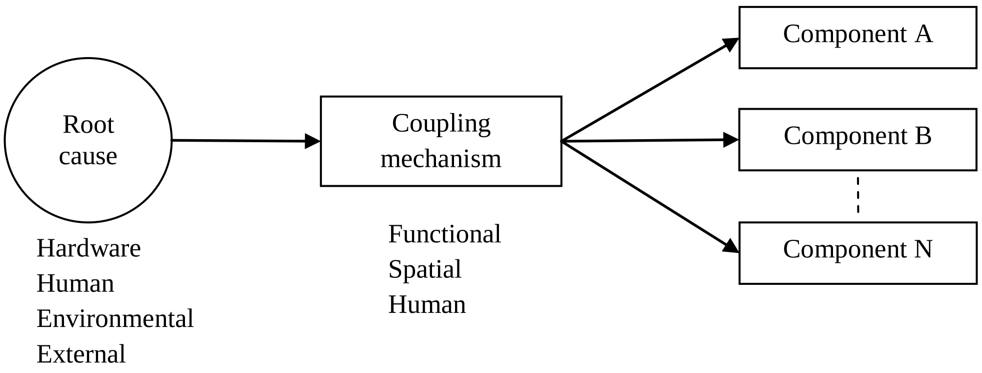


Fig. 2.1 Physical elements of a dependent event (NUREG/CR-4780, 1988)

In addition, (NUREG/CR-6819, 2003), suggests four criteria that should be met to consider an event as a CCF, that are:

- Two or more individual components fail, or are *degraded* (including failures during demand or in-service testing), or have deficiencies that would result in component failures if a demand signal had been received,
- Components fail within a selected period of time such that success of probabilistic risk assessment (PRA) mission would be uncertain,
- Components fail because of a *single shared cause mechanism* and coupling mechanism,
- Components fail within the established component boundary.

2.1 Common cause failures' parametric models

The major impact of CCFs on the redundant systems' reliability and availability is undeniable. This fact creates the unavoidable need to adopt an efficient strategy to manage this type of events within the reliability and risk analysis framework. In line with the current risk assessment practice, treating the CCF events requires the quantification of their probabilities, which is a rather complicated task. To deal with this issue, a large number of models have been proposed most of them are known as *parametric models*. The flowchart presented in Fig. 2.2 (taken from (NEA/ CSNI/ R (92) 18, 1993)) summarizes the most used ones.

At this point it seems useful to mention that the parametric models are frequently classified into shock and non-shock. The shock models recognize two failure mechanisms (NEA/ CSNI/ R (92) 18, 1993):

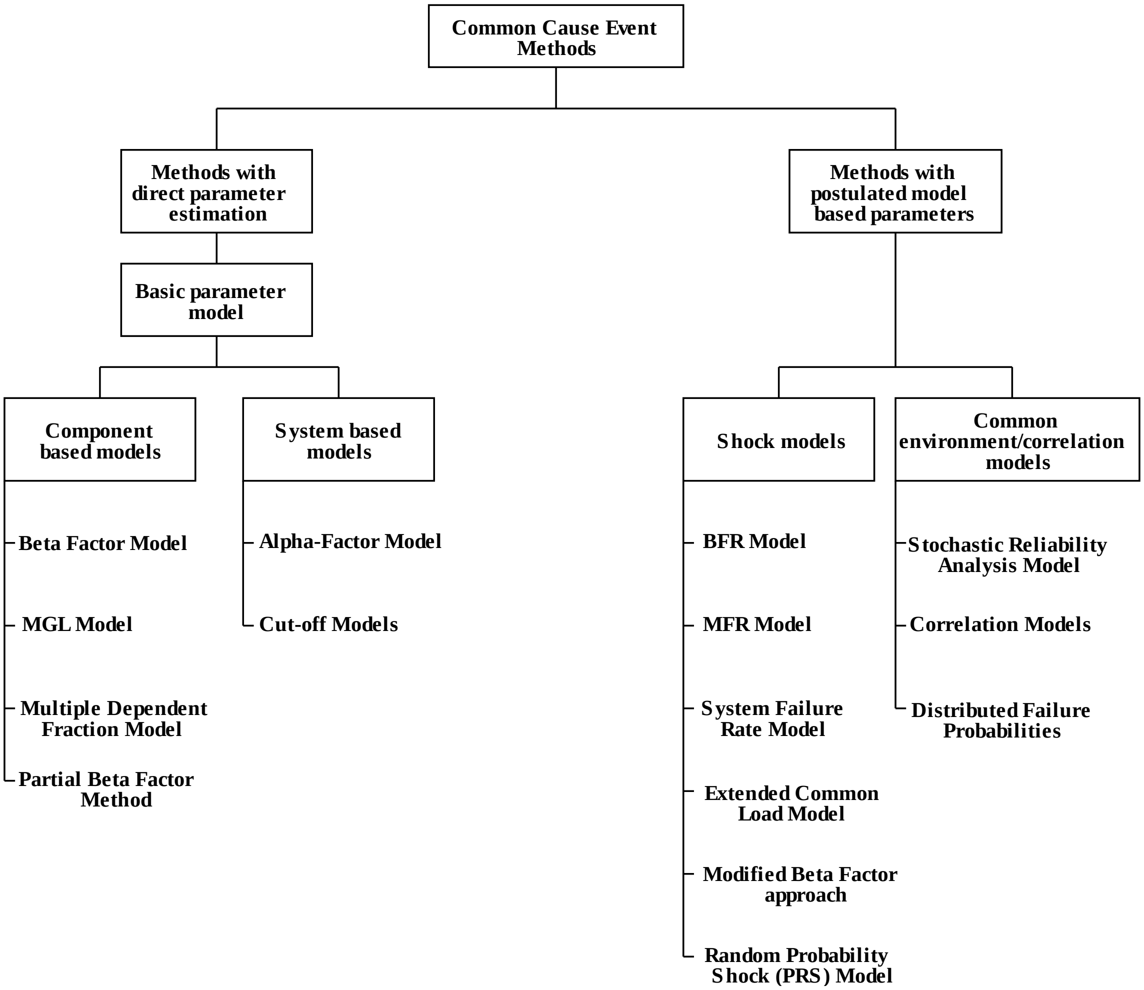
(1) failures due to random independent causes of single component failures and;
(2) failure of one or more components due to common cause shocks witch impact the system at a certain frequency.

Otherwise, the non-shock models do not make any distinction between independent and dependent failures for single failure event (Hokstad, 1993).

By assuming that the probabilities of similar events involving the same kind of components are identical (symmetry assumption), it is ordinary to consider Q_k^m as the probability of a basic event involving k specific components in a *common cause component group* (CCCG) of size m, $(1 \leq k \leq m)$ (Fleming, et al., 1985). As an illustration, Q_2^3 represents the probability of a basic event that hit two among the three elements. Moreover, the total failure probability Q_t of a component in a CCCG of size *m* is given by the subsequent equation:

$$Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k^m = \sum_{k=1}^{m} \frac{(m-1)!}{(k-1)!\,(m-k)!} Q_k^m \tag{2.2}$$

Those basic event probabilities can be estimated directly from data (if available) and without the intervention of any other parameters. This method is known as *basic parameter model* and it was introduced in (Fleming, et al., 1985). In what follows some of the most commonly used parametric models were selected to be more detailed.



Common Cause Event Methods
Methods with direct parameter estimation
Methods with postulated model based parameters
Basic parameter model
Component based models
System based models
Shock models
Common environment/correlation models
Beta Factor Model
MGL Model
Multiple Dependent Fraction Model
Partial Beta Factor Method
Alpha-Factor Model
Cut-off Models
BFR Model
MFR Model
System Failure Rate Model
Extended Common Load Model
Modified Beta Factor approach
Random Probability Shock (PRS) Model
Stochastic Reliability Analysis Model
Correlation Models
Distributed Failure Probabilities

Fig. 2.2 Assignment of common cause models to different classes (NEA/ CSNI/ R (92) 18, 1993)

2.1.1 Beta Factor model

This model forms with the *C Factor model* (see (Evans, et al., 1984; Parry, 1987)) the so-called *single parameter models*, wherein only one parameter (other than the total failure probability) is involved. Firstly introduced in (Fleming, 1975), the Beta Factor model is one of the most commonly used parametric models due to its simplicity and ease of understanding. It is also used in the IEC 61508 standard (IEC 61508, 2010), where an approach based on a checklist is used to estimate the related parameter.

The well-known limitation of this model lies in its inadequacy with the highly redundant systems ($m > 2$). This limitation comes from the assumption that considers the occurrence of a common cause failure would inevitably lead to the failure of all the CCCG elements. In other words:

$$Q_k^m = \begin{cases} (1-\beta)Q_t \ , k \ = \ 1 \\ 0 \ \ , 1 < k < m \\ \beta Q_t, \quad \text{otherwise} \end{cases} \tag{2.3}$$

2.1.2 Multiple Greek Letter (MGL) model

Originally suggested in (Fleming, et al., 1983), the Multiple Greek Letter model (MGL), which belongs to the non-shock category, uses a number of (m-1) parameters represented by the Greek letters ($\beta, \gamma, \delta, \ldots$). Those parameters describe the conditional probabilities of a double, triple, quadruple… failure given that a failure has occurred (NEA/ CSNI/ R (92) 18, 1993). The basic event probabilities according to the MGL model are expressed as:

$$Q_k^m = \frac{1}{\binom{m-1}{k-1}} \left(\prod_{i=1}^{k} \rho_i \right) (1 - \rho_{k+1}) \, Q_t \tag{2.4}$$

where,

$\rho_1 = 1, \rho_2 = \beta, \rho_3 = \gamma, \ldots, \rho_{m+1} = 0$

2.1.3 Alpha Factor model

The Alpha Factor model (Mosleh, et al., 1987) is another non-shock and multi-parameter model. The main advantage of this model lies in how to estimate the corresponding parameters. While the calculation of the other models' parameters such as MGL and Beta Factor model is based on the component failure data, the parameters of this latter are estimated directly from the system failure data (see the flowchart in Fig. 2.2). Even further, some estimation approaches employ the Alpha model parameters to approximate those of the MGL. In brief, the following equation relates the basic event probabilities to the Alpha Factor model parameters.

$$Q_k^m = \frac{k}{\binom{m-1}{k-1}} \, \frac{\alpha_k}{\alpha_t} \, Q_t \qquad k = 1, \ldots, m \tag{2.5}$$

where $\alpha_t \equiv \sum_{k=1}^{m} k\ \alpha_k$. And of course α represents the fraction of the events (CCFs) that occur in the system.

2.1.4 Binomial Failure Rate (BFR) model

As a shock model, the Binomial Failure Rate model (NUREG/CR- 2098, 1983) differentiates between the independent failures and those caused by shocks that can hit any number of elements within the CCCG. Furthermore, the shock failures are classified into lethal and nonlethal. The effects of the lethal ones involve all the components, while each component within the CCCG is assumed to have a constant and independent probability of failure in the nonlethal case (NUREG/CR-4780 (2), 1989). The relevant equation is shown next.

$$Q_k^m = \begin{cases} Q_I + \rho(1-\rho)^{m-1} & k = 1 \\ \mu\,\rho^k\,(1-\rho)^{\,m-k} & k \neq 1, m \\ \mu\,\rho^m + \omega & k = m \end{cases} \tag{2.6}$$

Where, Q_I is the independent failure frequency for each component, μ, ω are the frequencies of the occurrence of nonlethal and lethal shocks and ρ represents the conditional failure probability of each component, given that a nonlethal shock has occurred.

2.1.5 Multiple Beta Factor (MBF) model

This model has been introduced in (Hokstad, et al., 2003; Hokstad, et al., 2004), which is in fact an extension of the traditional Beta Factor model. Its contribution lies in taking into consideration the difference between the various logic configurations of a specific CCCG by adding the C_{MooN} coefficient as shown in Eq. (2.7).

$$\beta(MooN) = \beta \cdot C_{MooN}, (M < N) \tag{2.7}$$

where β is the same factor used in the original model and C_{MooN} is a modification factor for various voting configurations that could be obtained from Table 2.1 (Hokstad, et al., 2004):

Table 2.1 Modification factors, C_{MooN}, based on system voting logic

Voting	**1oo2**	**1oo3**	**2oo3**	**1oo4**	**2oo4**	**3oo4**
$\boldsymbol{C_{MooN}}$	1.0	0.3	2.4	0.15	0.8	4.0

In order to compute the Q_k^m using this model, we can rewrite the equation given in (Hokstad, et al., 2006) in the following manner:

$$Q_k^m = \beta Q_t \sum_{i=0}^{m-k} (-1)^i \binom{m-k}{i} \prod_{l=2}^{k-1+i} \beta_l \qquad k = 2, \dots, m \tag{2.8}$$

For the independent failures (k=1), we propose the following equation that is derived from Eq. (2.2):

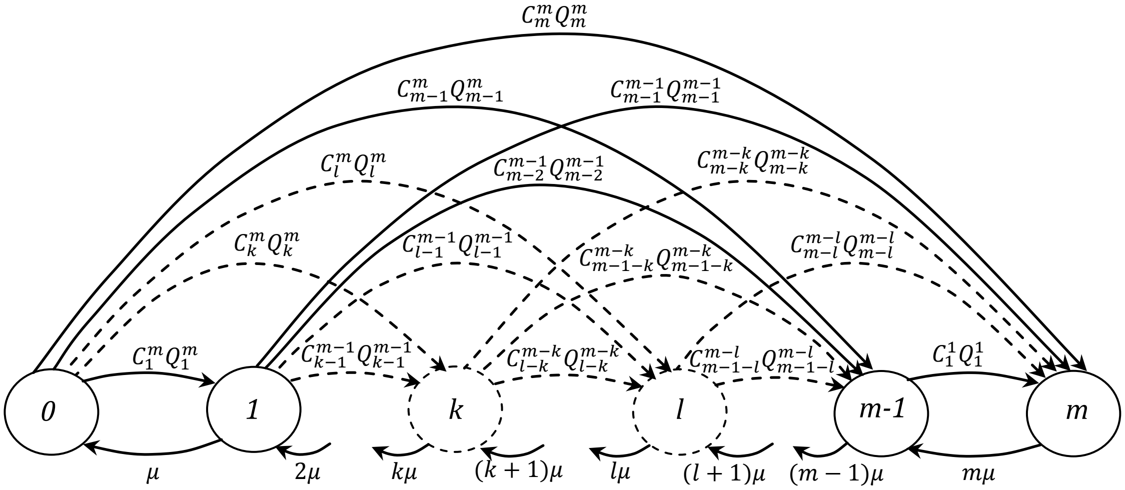
$$Q_1^m = Q_t - \sum_{k=2}^{m} \binom{m-1}{k-1} Q_k^m \tag{2.9}$$

In addition to the aforementioned models, many other ones have been created, combined and even modified in purpose of filling gaps within those conventional models. For example, the Trinomial Failure Rate model (TFR) has been suggested in (Han, et al., 1989) to take into consideration another component state called "*gray"* in addition to the two other classical ones (success and failure). This added state represents events such as incipient, partial and potential failures, which occur in practice and their ignorance may lead to underestimation or overestimation in the overall results. Furthermore, in the UK, an expert judgment based model has been developed to deal with CCFs called unified partial method (UPM). According to (Zitrou, et al., 2007) the superiority of this method over the other ones lies in its ability to model the impact of managerial, design and environmental defense factors on the CCF likelihood. It remains to clarify that describing in details all of the suggested methods over the past few decades to treat common cause failures is beyond the objectives of this essay, instead a quick overview of some of them is quite enough for the next task.

2.2 Unification of the parametric models

Because each parametric model has its own specifications, it is necessary to guarantee the proper application of these models and why not facilitate the transition between them. That is the ambition of the current section. For this end, the Markovian approach has been used. Its principle is abundantly treated in the literature and therefore is not detailed further in this work. We just notice that this approach has proven its effectiveness in terms of reliability and safety analysis for many decades and does not need any arguments or praises. This is largely due to its capability to consider certain event's dependencies. In this context, we may quote the following sentences that are taken from (Cantarella, 1989): "*The Markovian model applied to reliability analysis is well known as an effective tool, whenever some dependencies affect the probabilistic behavior of system's components. This is due, as we will see, to the perfect model's ability to integrate conditional failure and repair rates, according to the different system's states. Moreover, studying dynamical evolution of systems, we are able to include human actions into the temporal evolution*". Such dynamicity exists in our case, because the occurrence of CCF events modifies the failure behavior of the considered system. Often, that dynamicity cannot be correctly handled by conventional reliability methods (except the case where CCF are modeled through the Beta Factor model). The main objective of this section is to develop one Markov model that unifies the different CCF parametric models for any given system consists of any number of identical components. Then it is possible to study the impact of each single model on reliability and safety represented by their metrics, namely: a) average unavailability (U_{avg}), which is the complement of the availability that is defined in the previous chapter, and b) average unconditional failure intensity (failure frequency) (w_{avg}), where $w(t)dt$ represents the probability that an item fails at ($t, t + \Delta t$], given that it was operating at time zero. By the way, it is important to distinguish between this latter metric and the formerly seen failure density f (t), which is exclusively related to the occurrence of the first failure. However, they are identical only for the non-repairable items. This latter fact raises the opportunity for quantitatively comparing those parametric models.

Fig. 2.3 shows our proposition to unify the parametric models using Markovian graphs.



$C_m^m Q_m^m$
$C_{m-1}^m Q_{m-1}^m$
$C_{m-1}^{m-1} Q_{m-1}^{m-1}$
$C_l^m Q_l^m$
$C_{m-2}^{m-1} Q_{m-2}^{m-1}$
$C_{m-k}^{m-k} Q_{m-k}^{m-k}$
$C_k^m Q_k^m$
$C_{l-1}^{m-1} Q_{l-1}^{m-1}$
$C_{m-1-k}^{m-k} Q_{m-1-k}^{m-k}$
$C_{m-l}^{m-l} Q_{m-l}^{m-l}$
$C_1^m Q_1^m$
$C_{k-1}^{m-1} Q_{k-1}^{m-1}$
$C_{l-k}^{m-k} Q_{l-k}^{m-k}$
$C_{m-1-l}^{m-l} Q_{m-1-l}^{m-l}$
$C_1^1 Q_1^1$
0
1
k
l
m-1
m
μ
2μ
$k\mu$
$(k+1)\mu$
$l\mu$
$(l+1)\mu$
$(m-1)\mu$
$m\mu$

Fig. 2.3 Unified Markov model for the CCF parametric models

In Fig. 2.3, state 0 represents the successful operation of all the components, state 1 means that one component out of the m has failed and so on until the state m which represents the failure of all the CCCG's elements. The failure probability which accompanies the forward transition arc from any given state k to any other one l for $(k < l)$ is expressed by the multiplication of C_{l-k}^{m-k} by Q_{l-k}^{m-k}. The term C_{l-k}^{m-k} is the combination coefficient, which shows the number of the possible ways that a group of $l - k$ components out of $m - k$ fails, whilst Q_{l-k}^{m-k} is the same term already used in Section 2.1 (i.e., the probability of a basic event involving $l - k$ specific components in a common cause component group of size $m - k$) which can be calculated using one of the various CCF models. To simplify, it is assumed that all the failures are immediately detected and repaired according to a constant repair rate μ. It is also assumed that the number of the available repairmen is always sufficient. However, modifying the repairing policy or even adding more failure modes (e.g., undetected failures) is definitely possible.

2.3 Illustrative example

Let us consider an example of a Motor Driven Pump which is described in (CCF Parameter Estimations 2010, 2012), where data for the Beta Factor model, MGL model and Alpha Factor model is presented. If we suppose that the system consists of four components (Pumps), its corresponding Markov model would be as shown in Fig. 2.4.

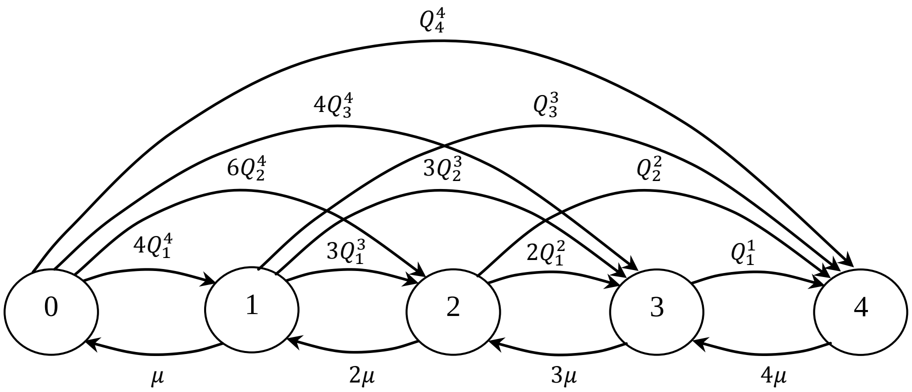


Fig. 2.4 Unified Markov model for a system of four components

Table 2.2 gathers the values of the different Q_k^m using data from the previously cited reference and the equations of each parametric model (see Section 2.1). It should be noted that the different Q_k^m are treated as failure rates. For calculation purposes, we suppose that $Q_t = 2.5E - 5\ h^{-1}$ and $\mu = 0.125\ h^{-1}$ (Mean Time to Repair (*MTTR*) = 8 *h*). For the MBF model we have taken the base case values (i.e., $\beta_2 = 0.3$ and $\beta_3 = 0.5$ (see (Hokstad, et al., 2004)).

The next step will allow us to clearly illustrate the difference between the four parametric models and the significance of that on the systems' dependability. The comparison is performed for the different *M*oo*N* (M-out-of-N) architectures that share this number of components (i.e., *N*=4). Of course, the same unified Markov model presented in Fig. 2.4 can be used for all those architectures by just specifying their respective working and failed states in the model.

Table 2.2 Values of the failure rates obtained by using different parametric models

Failure rates (h^{-1})	**Beta Factor model**	**MGL model**	**Alpha Factor model**	**MBF model**
Q_1^4	2.44325E-5	2.44325E-5	2.35721E-5	2.37231E-5
Q_2^4	0	1.04231E-7	2.00997E-7	3.12125E-7
Q_3^4	0	5.46987E-8	1.58225E-7	8.51250E-8
Q_4^4	5.67500E-7	9.07115E-8	3.50217E-7	8.51250E-8
Q_1^3	2.44225E-5	2.44225E-5	2.36457E-5	2.40183E-5
Q_2^3	0	1.68053E-7	3.26770E-7	4.04250E-7
Q_3^3	5.77500E-7	2.41395E-7	7.00739E-7	1.73250E-7
Q_1^2	2.43875E-5	2.43875E-5	2.38043E-5	2.43875E-5
Q_2^2	6.12500E-7	6.12500E-7	1.19570E-6	6.12500E-7
Q_1^1	2.50000E-5	2.50000E-5	2.50000E-5	2.50000E-5

2.3.1 1oo4 architecture

For the 1oo4 configuration, the system is unavailable only in state 4. By inserting the data of Table 2.2 in the related unified Markov model, we can easily estimate the different values of U_{avg} and w_{avg} of this architecture for a specific amount of time that equals one year (T = 8760 h). Eqs. (2.10) and (2.11) show the related U_{avg} and w_{avg} formulas, while the obtained results are summarized in Table 2.3. Furthermore, Figs. 2.5 and 2.6 depict the evolution of $U(t)$ and $w(t)$.

$$U_{avg}^{1oo4} = \frac{1}{T}\int_0^T P_4\,(t)\,\mathrm{d}t \tag{2.10}$$

$$w_{avg}^{1oo4} = \frac{1}{T}\int_0^T w(t)\,\mathrm{d}t = \frac{1}{T}\int_0^T [\,P_0(t)\cdot Q_4^4 + P_1(t)\cdot Q_3^3 + P_2(t)\cdot Q_2^2 + P_3(t)\cdot Q_1^1]\,\mathrm{d}t \tag{2.11}$$

where $P_i(t)$ is the probability of being in state i at the instant t.

Table 2.3 U_{avg} and W_{avg} for the 1oo4 architecture

	$\boldsymbol{U_{avg}}$	$\boldsymbol{w_{avg}}$
Beta Factor model	1.1348E-6	5.6754E-7
MGL model	1.8166E-7	9.0853E-8
Alpha Factor model	7.0094E-7	3.5056E-7
MBF model	1.7041E-7	8.5227E-8

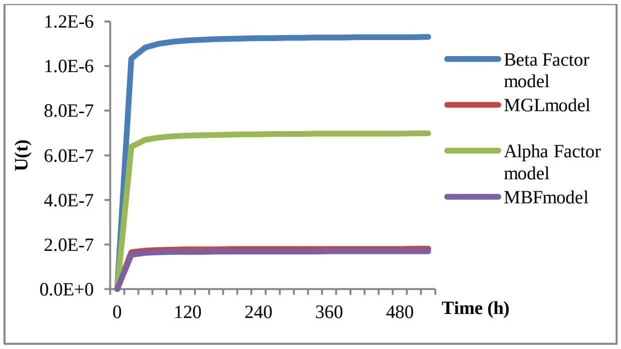


Fig. 2.5 $U(t)$ for 1oo4 configuration

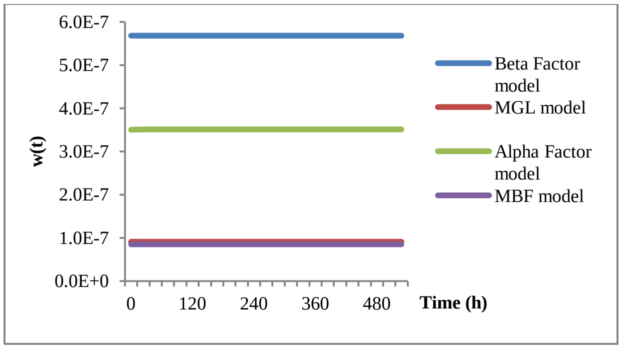


Fig. 2.6 $w(t)$ for 1oo4 configuration

The examination of Figs. 2.5 and 2.6 clearly shows that, for this architecture, the Beta Factor model offers the highest values for both U_{avg} and w_{avg}, while the MGL and MBF models that appear almost identical offer the two lowest ones.

2.3.2 2oo4 architecture

The same work is done for the 2oo4 configuration where the system is unavailable in state 3 as well as state 4 (see Eqs. (2.12) and (2.13)). For the same amount of time we get the results that are gathered in Table 2.4 and Figs. 2.7 and 2.8.

$$U_{avg}^{2oo4} = \frac{1}{T}\int_0^T [P_3\,(t) + P_4(t)]\,\mathrm{d}t \tag{2.12}$$

$$w_{avg}^{1oo4} = \frac{1}{T}\int_0^T w(t)\,\mathrm{d}t = \frac{1}{T}\int_0^T [\,P_0(t)\cdot(Q_4^4{+}4Q_3^4) + P_1(t)\cdot(Q_3^3 + 3Q_2^3) + P_2(t)\cdot(Q_2^2 + 2Q_1^2) + P_3(t)\cdot Q_1^1]\,\mathrm{d}t \tag{2.13}$$

Table 2.4 U_{avg} and W_{avg} for the 2oo4 architecture

	$\boldsymbol{U_{avg}}$	$\boldsymbol{w_{avg}}$
Beta Factor model	2.6477E-6	5.6763E-7
MGL model	1.0080E-6	3.0999E-7
Alpha Factor model	3.3241E-6	9.8408E-7
MBF model	1.3082E-6	4.2683E-7

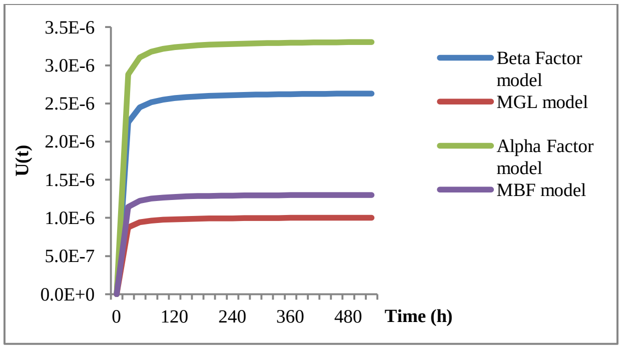


Fig. 2.7 $U(t)$ for 2oo4 configuration

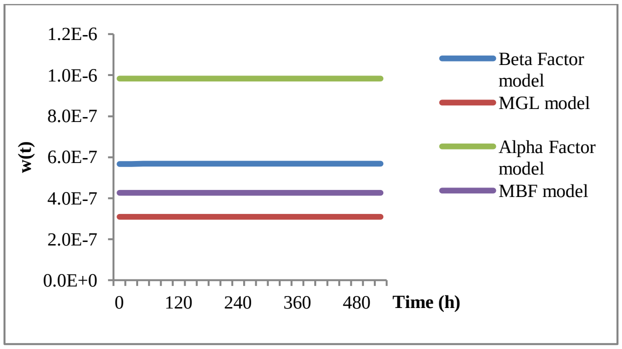


Fig. 2.8 $w(t)$ for 2oo4 configuration

This time the order is fairly different, unlike the case of 1oo4, the model that provides the highest U_{avg} and w_{avg} values is the Alpha Factor one, while the Beta Factor model comes in the second order. Although, the difference between the MGL and the MBF models is bigger this time, they remain far from the other two ones.

2.3.3 3oo4 architecture

For the 3oo4 architecture, the system is unavailable in three different states that are 2, 3 and 4. The subsequent results are obtained by using Eqs. (2.14) and (2.15), for the same amount of time (*T*= 8760 h).

$$U_{avg}^{3oo4} = \frac{1}{T}\int_0^T [P_2(t) + P_3\,(t) + P_4(t)]\,\mathrm{d}t \tag{2.14}$$

$$w_{avg}^{3oo4} = \frac{1}{T}\int_0^T w(t)\,\mathrm{d}t = \frac{1}{T}\int_0^T [\,P_0(t)\cdot(Q_4^4+4Q_3^4 + 6Q_2^4) + P_1(t)\cdot(Q_3^3 + 3Q_2^3+3Q_1^3) + P_2(t)\cdot(Q_2^2\ + 2Q_1^2) + P_3(t)\cdot Q_1^1]\,\mathrm{d}t \tag{2.15}$$

Table 2.5 U_{avg} and w_{avg} for the 3oo4 architecture

	U_{avg}	w_{avg}
Beta Factor model	5.1454E-6	6.2502E-7
MGL model	4.9757E-6	9.9247E-7
Alpha Factor model	1.2292E-5	2.2433E-6
MBF model	1.0718E-5	2.3536E-6

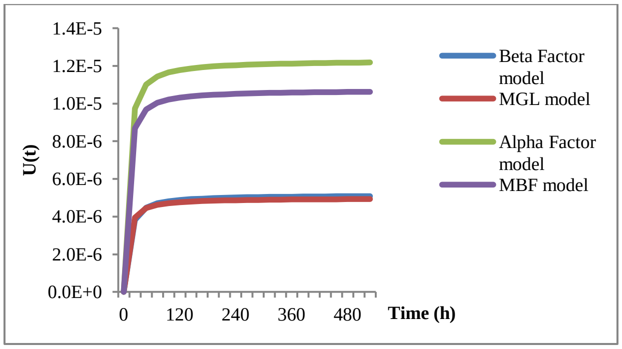


Fig. 2.9 $U(t)$ for 3oo4 configuration

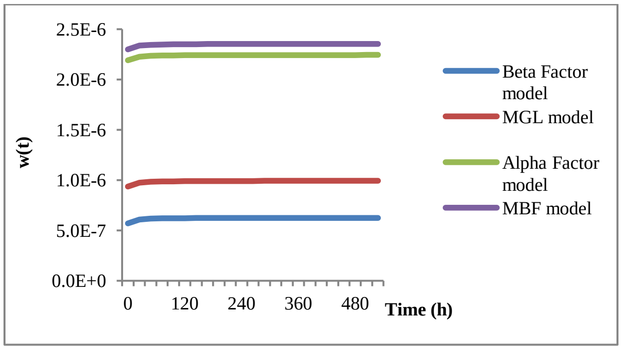


Fig. 2.10 $w(t)$ for 3oo4 configuration

Once again, the results are totally dissimilar to the past two architectures. In addition, we note the new dissimilarity between U_{avg} and w_{avg} in terms of the parametric models' order. This time as illustrate Figs. 2.9 and 2.10, it is so noticeable that the MBF model has jumped to offer the highest w_{avg} value and the second highest U_{avg} value after the Alpha Factor model. The other remarkable issue is that the Beta Factor model is giving absolutely the lowest w_{avg} value, while it becomes a bit near to the MGL model with respect to U_{avg}.

2.3.4 4oo4 architecture

In case of the 4oo4 architecture, the system is unavailable in all of the states 1, 2, 3 and 4. Table 2.6 contains the different values of U_{avg} and w_{avg} derived according to Eqs. (2.16) and (2.17).

$$U_{avg}^{4oo4} = \frac{1}{T}\int_0^T [P_1(t) + P_2(t) + P_3\,(t) + P_4(t)]\,\mathrm{d}t \tag{2.16}$$

$$w_{avg}^{4oo4} = \frac{1}{T}\int_0^T w(t)\,\mathrm{d}t = \frac{1}{T}\int_0^T [\,P_0(t)\cdot(Q_4^4{+}4Q_3^4 + 6Q_2^4 + 4Q_1^4) + P_1(t)\cdot(Q_3^3 + 3Q_2^3{+}3Q_1^3) + P_2(t)\cdot(Q_2^2 + 2Q_1^2) + P_3(t)\cdot Q_1^1]\,\mathrm{d}t \tag{2.17}$$

Table 2.6 U_{avg} and w_{avg} for the 4oo4 architecture

	$\boldsymbol{U_{avg}}$	$\boldsymbol{w_{avg}}$
Beta Factor model	7.9018E-4	9.8220E-5
MGL model	7.9294E-4	9.8587E-5
Alpha Factor model	7.8279E-4	9.6402E-5
MBF model	7.8691E-4	9.7114E-5

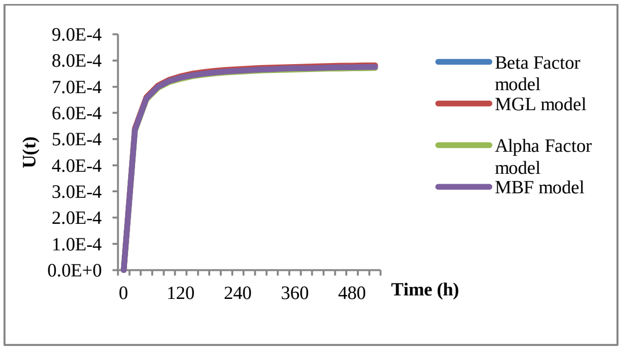


Fig. 2.11 $U(t)$ for 4oo4 configuration

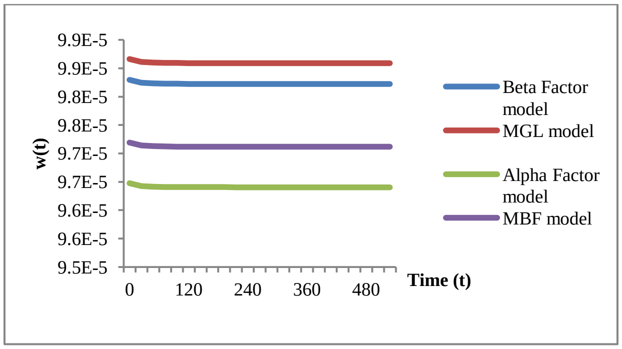


Fig. 2.12 $w(t)$ for 4oo4 configuration

From Table 2.6 and as substantiated by Figs. 2.11 and 2.12, the most noticeable matter for the case of 4oo4 architecture is the large convergence between the various parametric models. Also, for the first time the MGL model is providing the highest values for both U_{avg} and w_{avg} whereas the Alpha Factor model is producing the lowest ones. The order has returned to be the same for U_{avg} and w_{avg}.

2.4 Quantitative comparison between the Beta Factor model and MBF model

In the previously treated example, only the base case of the MBF model has been considered. In purpose of profoundly and fairly treat such model we dedicate this section to quantitatively compare the results it yields to those of the traditional Beta Factor model using the same metrics. In fact, the values of the factor C_{MooN} that are gathered in Table 2.1 are somehow general and they could be used to facilitate the employment of the MBF model. The estimation of such factor necessitates the intervention of a new factor denoted by β_p and represents the probability that a specific channel has failed given that p channels have failed. Furthermore, the estimation of this latter factor directly from data is generally inaccessible due to their shortage, the reason that led to suggest the following simplifications in (Hokstad, et al., 2006):

Case 1: $\beta_p = \beta_r$, for all $p \geq r$, this case in turn is split into two other sub-cases, namely: a) $\beta_p = \beta_2$, $p \geq 2$ and b) $\beta_p = \beta_3$, $p \geq 3$.

Case 2: $\beta_p = 1 - (1 - \beta_r) \cdot c^{p-r}$, where $p \geq r$ and "c" is a constant that may take any value from 0 through 1.

In what follows, a set of five *M*oo*N* architectures will be addressed that could be split according to *N* into two main classes, namely *N*=3 and *N*=4. Note that for *N*=2 the two models are identical, the reason that makes treating this case meaningless. For the whole calculation process, we made the following assumptions: constant failure rate for each component $Q_t = 2.5E-5\ h^{-1}$, $\beta = 2.27E-2$ and *T*=8760 *h*; failures are immediately detected and repaired according to a constant repair rate $\mu = 1/8 = 0.125\ h^{-1}$ (for each single component). Moreover, regarding the MBF model, different values for β_2 will be considered to cover its entire range, namely: 0.1, 0.3, 0.5 and 0.9, while the value of β_3 is fixed at 0.5 (of course for *N*=4) as it is suggested in (Hokstad, et al., 2006) and as it is mentioned in the same reference "*when the β_2 value has been chosen, the C_{MooN} values (N > 3) are not that sensitive to the choice of β_p (p ≥ 3)*". Actually, only case 1 will be considered in this comparison.

Additionally, to estimate U_{avg} and w_{avg}, it is required to employ Eq. (2.3) for the Beta Factor model and Eqs. (2.8) and (2.9) for the MBF one to obtain the different Q_k^m values, which are gathered in Table 2.7.

Table 2.7 The different Q_k^m values obtained by using the two parametric models

Q_k^m Models		Q_1^1	Q_1^2	Q_2^2	Q_1^3	Q_2^3	Q_3^3	Q_1^4	Q_2^4	Q_3^4	Q_4^4
Beta		2.5E-5	2.4432E-5	5.675E-7	2.4432E-5	0	5.675E-7	2.44325E-5	0	0	5.675E-7
MBF	0.1	2.5E-5	2.4432E-5	5.675E-7	2.3922E-5	5.1075E-7	5.6750E-8	2.3439E-5	4.8237E-7	2.8375E-8	2.8375E-8
	0.3	2.5E-5	2.4432E-5	5.675E-7	2.4035E-5	3.9725E-7	1.7025E-7	2.3723E-5	3.1212E-7	8.5125E-8	8.5125E-8
	0.5	2.5E-5	2.4432E-5	5.675E-7	2.4149E-5	2.8375E-7	2.8375E-7	2.4007E-5	1.4187E-7	1.4187E-7	1.4187E-7
	0.9	2.5E-5	2.4432E-5	5.675E-7	2.4376E-5	5.6750E-8	5.1075E-7	2.4574E-5	-1.9862E-7	2.5537E-7	2.5537E-7

2.4.1 Three components (*N*=3)

We can use here the Markov model presented in Fig. 2.4 by just eliminating state 4 and its related transitions. However, for this number of components, the studied architectures are 1oo3 and 2oo3. For the first architecture, the system is unavailable only in state 3, while for the 2oo3 it is unavailable in state 3 as well as state 2.

By inserting the $Q_1^1, Q_1^2, Q_1^3, Q_2^2, Q_2^3$ and Q_3^3 values in the corresponding Markov model we can get the results of the 1oo3 configuration that are presented in Table 2.8 and Figs. 2.13 and 2.14.

Table 2.8 U_{avg} and w_{avg} for the 1oo3 architecture

Dependability Metric Model			U_{avg}	w_{avg}
Beta Factor			1.5130E-6	5.6756E-7
MBF	β_2	0.1	1.5251E-7	5.7211E-8
		0.3	4.5484E-7	1.7062E-7
		0.5	7.5717E-7	2.8403E-7
		0.9	1.3618E-6	5.1085E-7

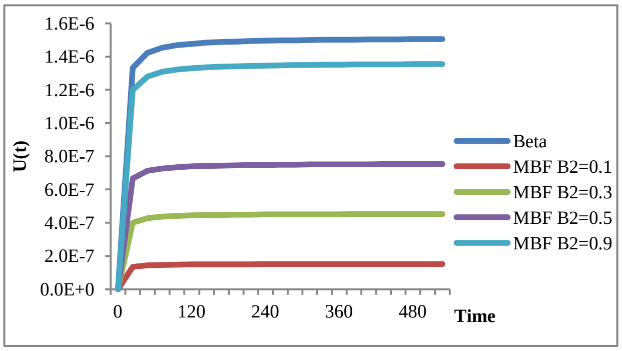


Fig. 2.13 $U(t)$ for 1oo3 configuration

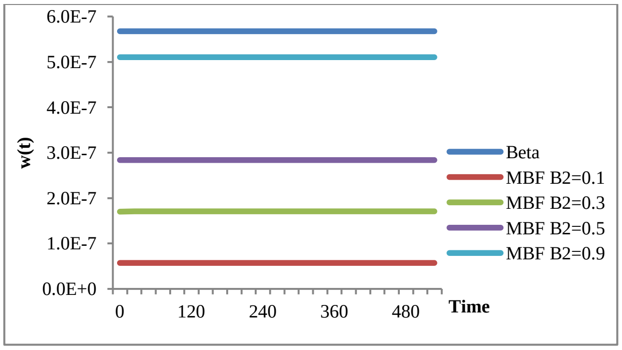


Fig. 2.14 $w(t)$ for 1oo3 configuration

Obviously, the Beta factor model gives the highest values for both U_{avg} and w_{avg} no matter what is the value of β_2. In addition, it is clear that as the value of this latter factor heightens the MBF model come close to the Beta Factor one, which is absolutely an expected conclusion. The relative variation (Δν/ν) between the Beta Factor model and the base case (i.e., β_2=0.3) of the MBF model equals 6.99E-1 for both metrics.

For the 2oo3 architecture, Table 2.9 and Figs. 2.15 and 2.16 show tits corresponding results derived from Beta Factor and MBF models.

Table 2.9 U_{avg} and w_{avg} for the 2oo3 architecture

Dependability Metric Model		U_{avg}	w_{avg}
Beta Factor		3.8965E-6	5.9633E-7
MBF β_2	0.1	6.6175E-6	1.6170E-6
	0.3	6.0128E-6	1.3902E-6
	0.5	5.4082E-6	1.1634E-6
	0.9	4.1989E-6	7.0974E-7

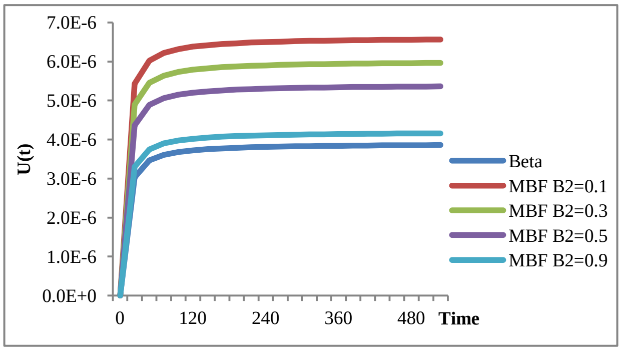


Fig. 2.15 $U(t)$ for 2oo3 configuration

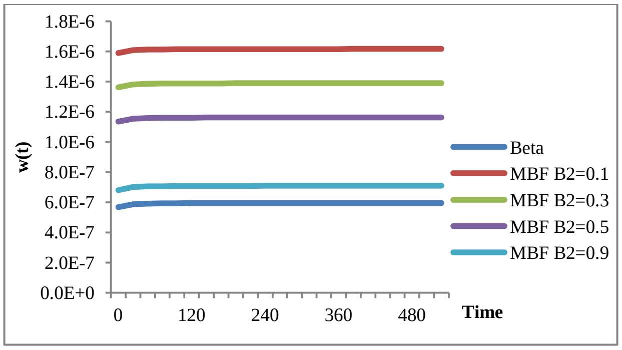


Fig. 2.16 $w(t)$ for 2oo3 configuration

Actually, the case of 2oo3 is quite different, since the Beta Factor model provides entirely the lowest values for the two dependability metrics, while the highest value of β_2 remains nearer to the Beta Factor model than the lowest one. The relative variation of the base case is -5.43E-1 for U_{avg} and -1.33 for w_{avg}.

2.4.2 Four components (*N*=4)

Concerning this case, three configurations will be taken into consideration, which are 1oo4, 2oo4 and 3oo4. Indeed, the Markov model presented in Fig. 2.4 could be used as it is here and all the Q_k^m values are calculated and gathered in Table 2.7. Of course, the factor β_3 is involved this time. Let us start with the 1oo4 configuration, which makes the system unavailable only in state 4. Table 2.10 and Figs. 2.17 and 2.18 give its related results.

Table 2.10 U_{avg} and w_{avg} for the 1oo4 architecture

Dependability Metric / Model			U_{avg}	w_{avg}
Beta Factor			1.1348E-6	5.6754E-7
MBF	β_2	0.1	5.6812E-8	2.8413E-8
		0.3	1.7041E-7	8.5224E-8
		0.5	2.8400E-7	1.4204E-7
		0.9	5.1120E-7	2.5566E-7

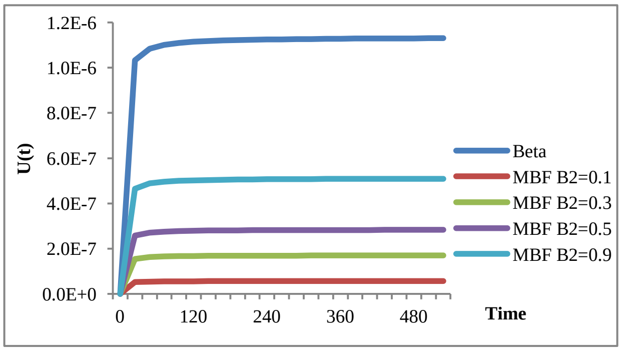


Fig. 2.17 $U(t)$ for 1oo4 configuration

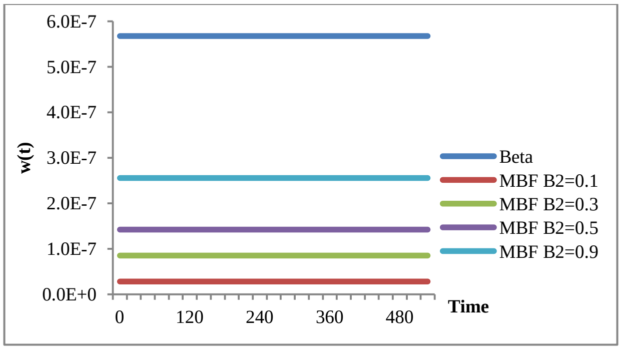


Fig. 2.18 $w(t)$ for 1oo4 configuration

It seems that the relationship between the two parametric models is similar to the 1oo3 case. The relative variation between the base case (i.e., β_2=0.3 and β_3=0.5) of the MBF model and the Beta Factor model equals 8.5E-1 for both U_{avg} and w_{avg}.

The turn goes now to the 2oo4 architecture that makes the system unavailable in state 4 as well as state 3. The relevant obtained results are shown in Table 2.11 and Figs. 2.19 and 2.20.

Table 2.11 U_{avg} and w_{avg} for the 2oo4 architecture

Dependability Metric Model			U_{avg}	w_{avg}
Beta Factor			2.6476E-6	5.6762E-7
MBF	β_2	0.1	4.3961E-7	1.4360E-7
		0.3	1.3082E-6	4.2681E-7
		0.5	2.1767E-6	7.1002E-7
		0.9	3.9144E-6	1.2767E-6

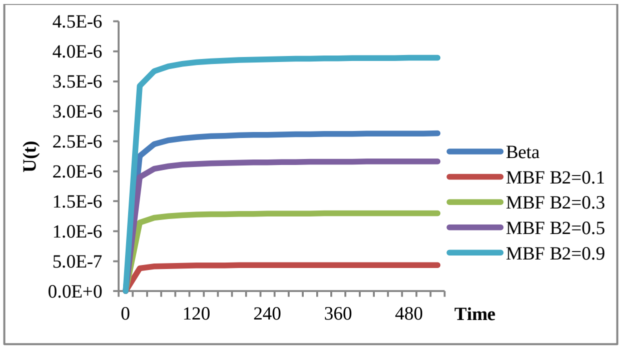


Fig. 2.19 $U(t)$ for 2oo4 configuration

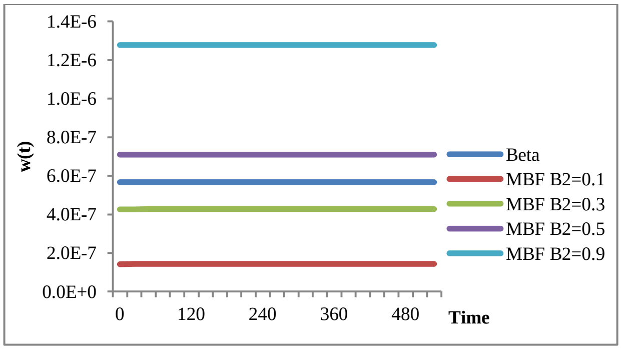


Fig. 2.20 $w(t)$ for 2oo4 configuration

For the 2oo4 architecture, the situation is completely different from any other precedent one. This time the highest values of U_{avg} and w_{avg} are provided by the MBF model with β_2=0.9 then the Beta Factor model comes in the second place just for U_{avg}, while for w_{avg} it is in the third place after the case of β_2=0.5. Furthermore, the relative variation is 5.06E-1 for U_{avg} and 2.48E-1 for w_{avg}.

At last, we arrive at the 3oo4 system which is unavailable in all of the states 4, 3 and 2. Subsequently, the results of the two metrics are given in Table 2.12 and Figs. 2.21 and 2.22.

Table 2.12 U_{avg} and w_{avg} for the 3oo4 architecture

Dependability Metric Model		$\boldsymbol{U_{avg}}$	$\boldsymbol{w_{avg}}$
Beta Factor		5.1454E-6	6.2504E-7
MBF β_2	0.1	1.2795E-5	3.0904E-6
	0.3	1.0718E-5	2.3536E-6
	0.5	8.6397E-6	1.6167E-6
	0.9	9.2483E-6	1.4375E-7

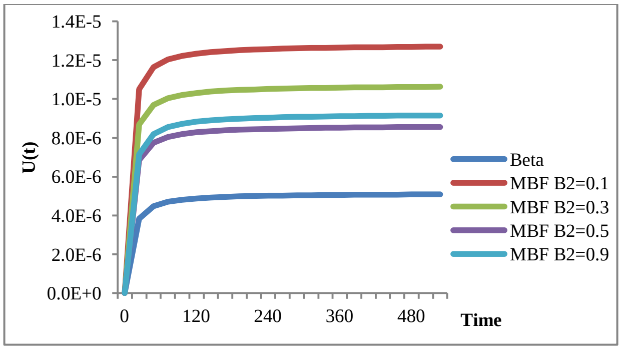


Fig. 2.21 $U(t)$ for 3oo4 configuration

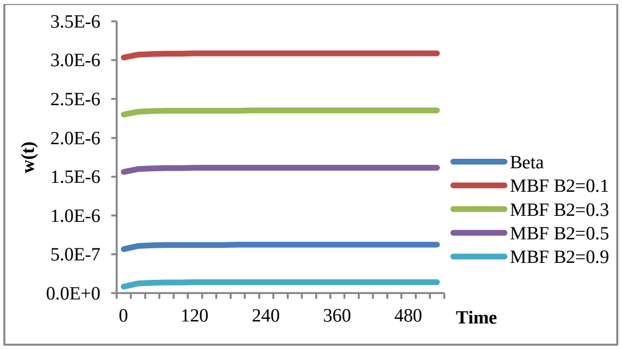


Fig. 2.22 $w(t)$ for 3oo4 configuration

For this latter architecture, the MBF model with β_2=0.1 and β_2=0.3 gives the two highest values for both U_{avg} and w_{avg}. The Beta Factor model comes at last for of U_{avg}, while this place is taken by the case of β_2=0.9 for w_{avg}. The relative variation equals -1.08 for U_{avg} and -2.48 for w_{avg}.

It is worth to notice that a general trend appears where the MBF model became conservative compared to the BF one when the required working elements M get closer to the total number of elements N: increasing the number of the failed states.

2.5 Conclusion

The biggest challenge within this chapter was finding a simple way that provides the supple use and integration of the different models that aim to treat the CCF events in the reliability and safety studies. For that purpose, we have developed a unified Markov model. In fact, the flexibility of the Markovian approach makes it the appropriate technique to reach that challenge. By using the proposed unified model, it is quite enough to estimate the failure probabilities or rates by means of any parametric model, the matter that makes this latter easier to implement and even to match up to many other alternatives.

Indeed, the studied architectures (1oo4, 2oo4, 3oo4 and 4oo4) in the first illustrative example have demonstrated that, regarding the order of U_{avg} and w_{avg} they provide, the performance of the parametric models is not the same for all the architectures. Moreover, the discrepancy between the different parametric models is very tiny for the case where $M = N$, due to the importance of the contribution related to the first independent event ($C_1^m \cdot Q_1^m$) compared to that of the CCFs events. For that reason, many authors prefer to not consider CCF events in reliability and safety studies for this special configuration (i.e., serial configuration), as it is the case of the IEC 61508 standard related to safety instrumented systems (IEC 61508, 2010).

Concerning the comparison between the Beta Factor and the MBF models, we have noticed that increasing the value of β_2 does not necessarily lead to making the MBF model nearer to the BF one, which is obvious in the case of 2oo4 and 3oo4 architectures. It should be noted also that even by choosing the β_2, the value of β_p for (p ≥ 3) could be significant. For example, the $w_{avg}$of 1oo4 for β_2=0.3 and β_3=0.5 equals 8.5224E-8 h^{-1} while it equals 1.0223E-7 h^{-1} by just taking β_3=0.6. Another unenthusiastic point regarding the MBF model is its haziness and mathematical complication especially for the user who has available data and wants to pass up the direct C_{MooN} values. A last odd thing concerning the MBF model is the negative sign in the obtained value of Q_2^4 for β_2=0.9 that maybe a mistake in our calculations even though with recalculating it several times with deferent ways as well as an error in the employed equation itself. To be evenhanded, we have to mention that the MBF model does extremely well when it comes to distinguishing between the performances of the different voting logics at least within the same number of components.

To sum up, it seems useful to cite that claiming that the Beta Factor model yields the most conservative results is just accurate when M=1 for any $M$oo$N$ configuration. What is more, for some architectures like 2oo3 and 3oo4 the situation is totally the opposite of the former claim. This study has demonstrated that the use of the Beat Factor model is advantageous, not only due to its simplicity (mathematical and data requirements) but also to the fact that the conservative character could be related to any other alternative.

3. IMPACT OF SAFE/DANGEROUS FAILURES ON SAFETY/OPERATIONAL INTEGRITY

Besides the quantitative way to determine the effects of the random failures, which relies principally on the estimation of the average probability of failure on demand (PFD_{avg}) for the low demand mode and the average probability of failure per hour (*PFH*) for the high and continuous demand modes, the IEC 61508 has introduced the concept of *architectural constraints* as another requirement for the hardware safety integrity of an E/E/PE safety-related system. This latter concept must be achieved by using one of two possible routes (1_H, 2_H). Route 1_H is based on the so-called *hardware fault tolerance* (*HFT*) ($N - K$ for a *KooN* architecture) and *safe failure fraction* (*SFF*). Such fraction is defined as "*property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures*" and it could be calculated using the subsequent equation:

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} \tag{3.1}$$

Obviously, the *SFF* concept somehow means that all of the safe failures, whether they are detected or not, and dangerous detected failures versus the dangerous undetected ones are advantageous for the safety integrity. Actually, this idea has not found a great acceptance, and the *SFF* validity and utility have been examined and criticized in several references, such as (Innal, 2008; Yoshimura, 2008; Lundteigen, et al., 2009). However, we stay in the use of PFD_{avg} and PFH and we look in the first section of this chapter at the correctness of neglecting the contribution of the safe failures in estimating such metrics. On the other hand, the second section is devoted to scrutinize the matter of neglecting the dangerous failures in the calculation of another type of SIS performance indicators that aim primarily to measure the operational integrity side, namely: a) the average probability of failing safely (PFS_{avg}) and b) spurious trip rate (*STR*). Such tasks will impose the need to describe the principles of the utilized architectures as well as their corresponding multi-phase Markov models. Actually, the quantitative application of these latter models is implemented within (GRIF, 2014) software.

3.1 Quantitative evaluation of safe failures' impact on the safety integrity

As it has been mentioned formerly, safety integrity is habitually measured by means of the average probability of failure on demand (PFD_{avg}) and the average probability of failure per hour (PFH), depending on the demand mode. In fact, these two performance indicators are the same used ones in the previous chapters. In other words, PFD_{avg} represents the average unavailability (U_{avg}) and PFH corresponds to the average unconditional failure intensity (failure frequency) (w_{avg}).

However, since the failure modes and according to their effects on the availability of the safety system and the EUC itself are categorized into safe and dangerous, it has been widely used and practically accepted to consider that only the dangerous failures have the potential to affect safety. In other words, safe failures, which specifically result in the false activation of the safety function and the spurious shutdown of the EUC, are completely neglected during the process of estimating those two metrics of the safety integrity.

On the other hand, several scientists and engineers believe that the safe failures have negative effects regarding the safety integrity, at least, when it comes to the process restoration conditions that can constitute an appropriate milieu for technical spoilages and human errors, which in turn may lead to more serious events. This matter has been pointed out in many references, such as (Goble, 1998 (b); Langeron, et al., 2007; Lundteigen, et al., 2008 (a); Lundteigen, et al., 2009).

In this section, the main objective is performing a deep quantitative evaluation of the impact of the safe failures on the safety integrity represented by the two metrics PFD_{avg} and PFH, employing multi-phase Markov models for some of the widely used *K*oo*N* architectures. In fact, this evaluation is an expansion of the study that has been conducted in (Dutuit, et al., 2009; Innal, 2008), where the values of λ_D and λ_S will be largely variegated and differentiated from each other and even further, different values will be assigned to the β factor of each type of failures to exhaustively take into consideration the possible effects of CCFs.

3.1.1 Modeling construction

At the beginning, two versions of multi-phase Markov models have been built for some of the commonly used *K*oo*N* architectures, in the first version the safe failures are included while in the other one are eliminated. The following step is comparing the different values of PFD_{avg} and PFH obtained from the two versions for each single configuration. It should be noted that the modeling assumptions are the same in the 6th part of (IEC 61508, 2010). It is assumed that all the channels are designed with the commonly used "*de-energized to trip*" concept (i.e., outputs energized during the normal operation of the process). Table 3.1 gathers the values of all the used parameters during the modeling process.

Table 3.1 Modeling parameters

Parameter	Value	
μ_{DD}, μ_{SD}	$(8)^{-1}$	h^{-1}
μ_r	$(24)^{-1}$	h^{-1}
T_1	8760	h
MT	43800	h
β_D, β_{SD}	$^{\beta}/_{2}, ^{\beta_S}/_{2}$	

- **1oo1 architecture**

The one-out-of-one architecture does not provide any fault tolerance, which means that the occurrence of one failure will cause the shutdown of the whole process spuriously, if the failure is safe, and disable the safety function if the failure is dangerous. The relevant electrical diagram and Markov model are presented in Figs. 3.1 and 3.2. States 2 and 3 represent the system dangerous failure states.

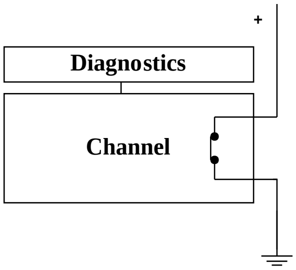


Fig. 3.1 1oo1 electrical diagram

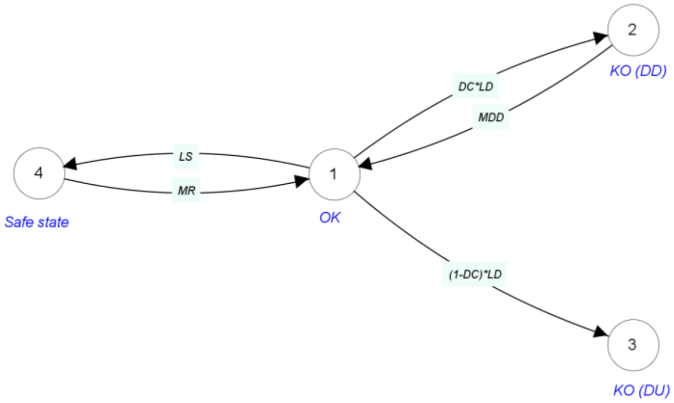


Fig. 3.2 1oo1 multi-phase Markov model

- **1oo2 architecture**

In this architecture two channels are wired in series. It provides high safety by tolerating the occurrence of a dangerous failure in one of the two channels. Unfortunately, it has a worse performance than the previous one when it comes to the spurious activation because it doubles the likelihood of having a nuisance trip. The dangerous failure states of the system are 4, 5 and 6.

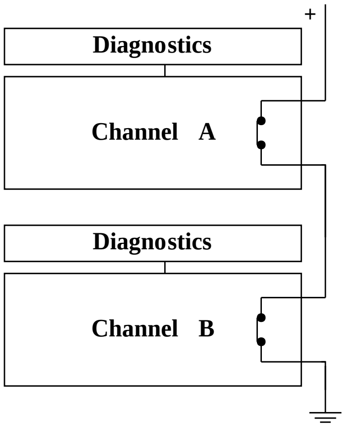


Fig. 3.3 1oo2 electrical diagram

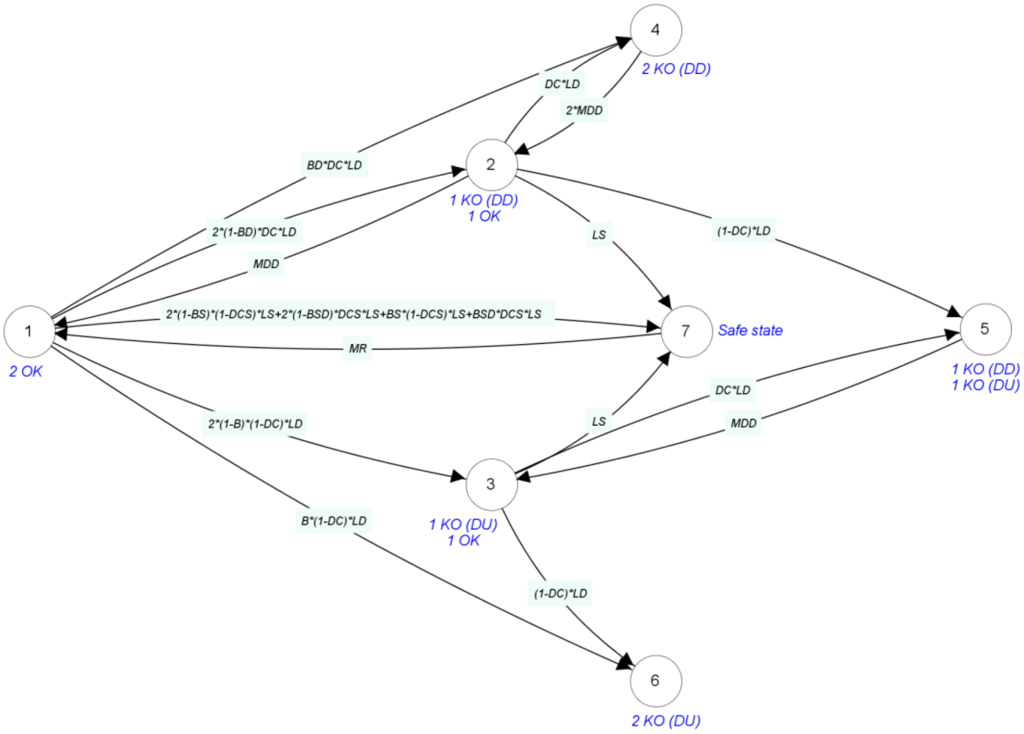


Fig. 3.4 1oo2 multi-phase Markov model

- **2oo2 architecture**

This configuration is composed of two channels wired in parallel. In fact, the two channels must fail safely to bring the system to the safe state, while only one dangerous failure can cause the loss of the safety function. All of the states 2, 3, 7, 8, 9, 10, 11, 12 and 13 characterize the system dangerous failure states.

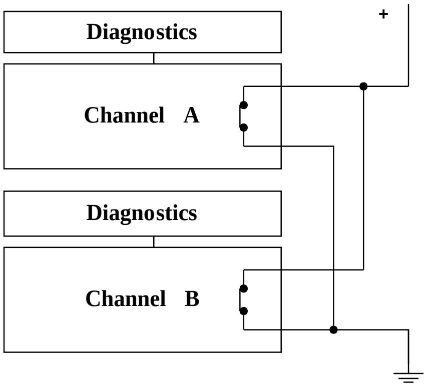


Fig. 3.5 2oo2 electrical diagram

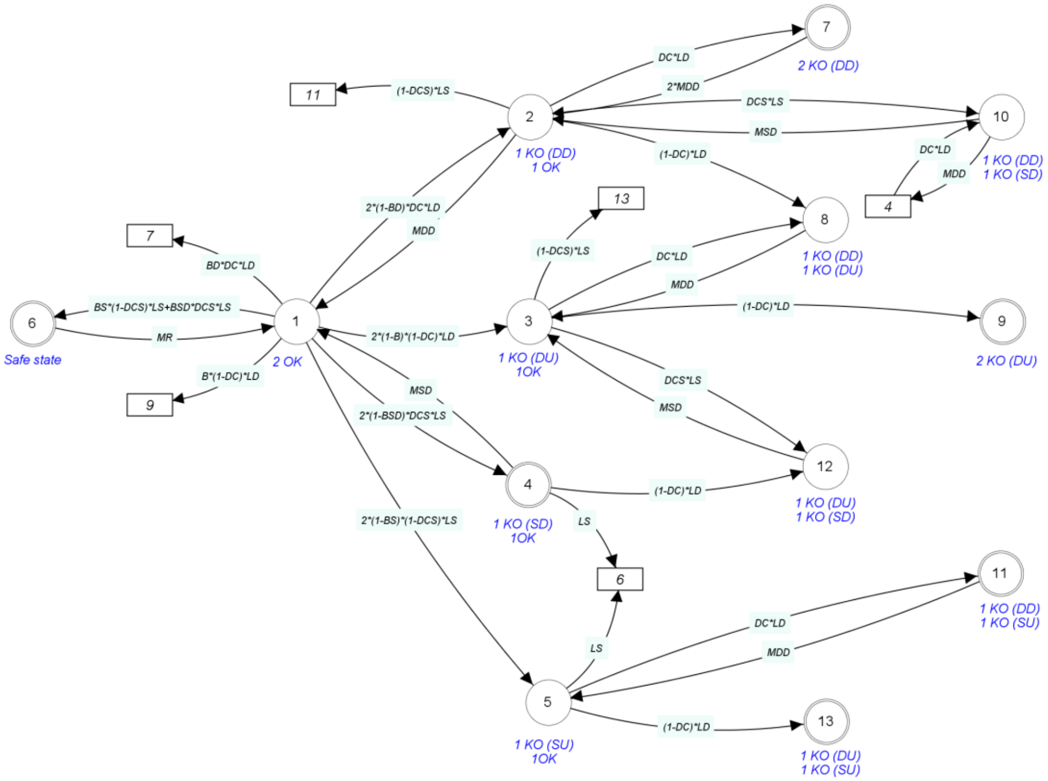


Fig. 3.6 2oo2 multi-phase Markov model

- **1oo2D architecture**

Similarly to the 2oo2, this architecture uses two channels wired in parallel. The 1oo2D is widely used since it reconciles safety and availability. Each diagnostic circuitry in this one has the ability to de-energize its channel when it detects the failure, which is not the case in the other five configurations studied here. Furthermore, additional control lines are added to allow each unit to de-energize the other one (Goble, 2010; Goble, et al., 2005). In the corresponding Markov model, there are five dangerous failure states that are: 5, 7, 8, 9 and 10.

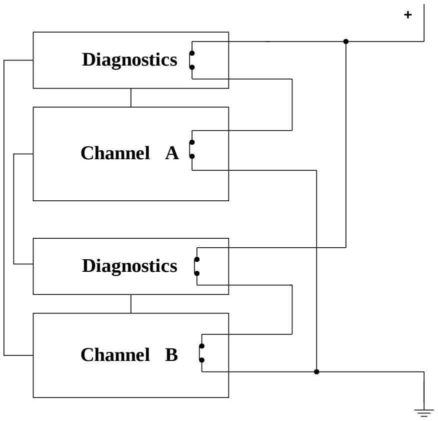


Fig. 3.7 1oo2D electrical diagram

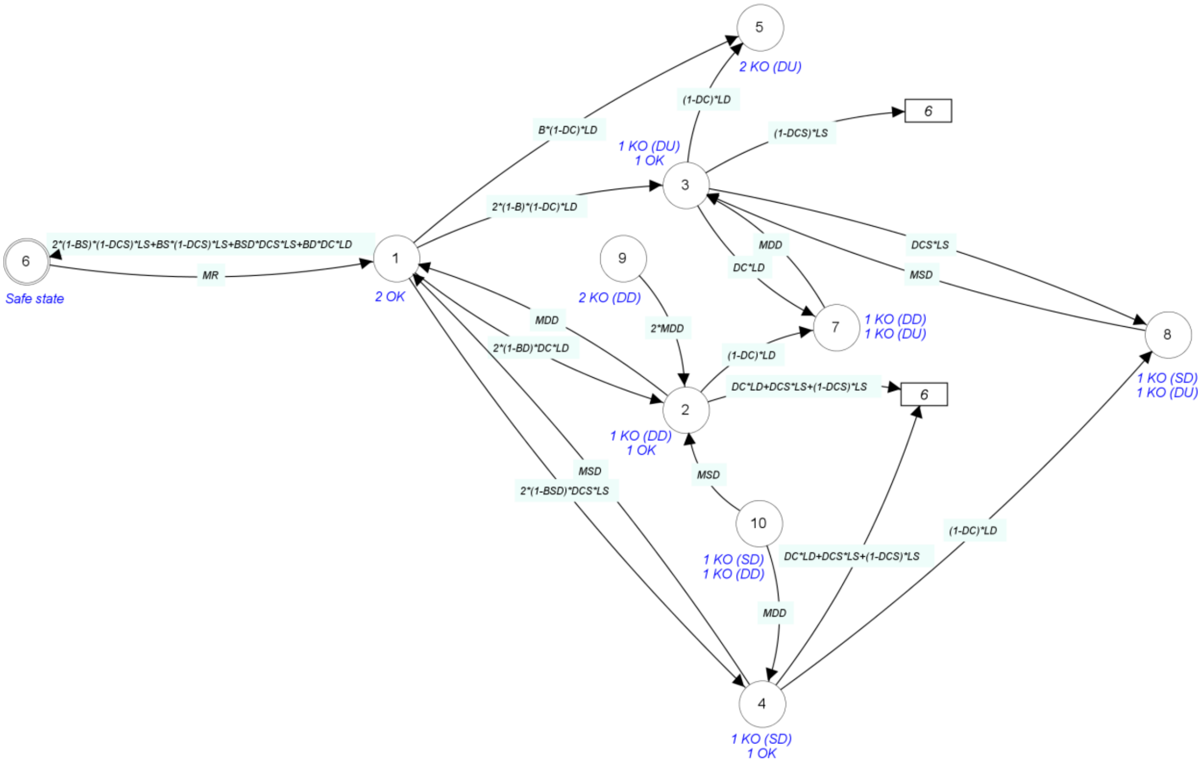


Fig. 3.8 1oo2D multi-phase Markov model

- **1oo3 architecture**

As illustrated in Fig. 3.9, the 1oo3 design is composed of three channels wired in series; this means that it is able to tolerate two dangerous failures at the same time. On the other hand, one safe failure can take the entire system (i.e., EUC) to the safe state. In Fig. 3.10, the dangerous failure states are: 7, 8, 9 and 10.

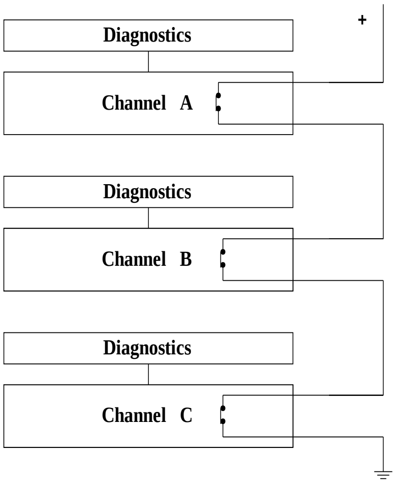


Fig. 3.9 1oo3 electrical diagram

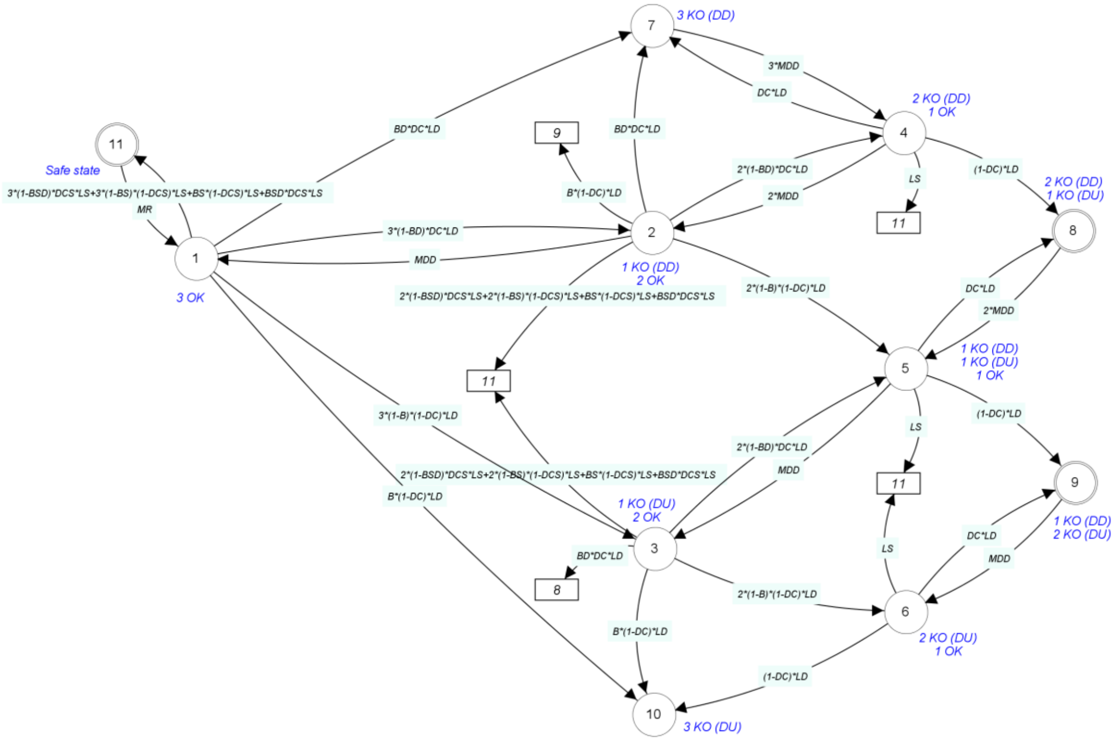


Fig. 3.10 1oo3 multi-phase Markov model

- **2oo3 architecture**

The 2oo3 architecture was developed to tolerate both safe and dangerous failures (Goble, et al., 2005; Goble, 2010). Two dangerous failures must occur to lose the safety function and at least two channels must fail safely in order to shutdown the process spuriously. The corresponding electrical diagram and Markov model are shown in Figs. 3.11 and 3.12. All of the states 4, 5, 6, 7, 8, 9, 10, 17, 18, 19, 20, 21 and 22 represent the system dangerous failure states.

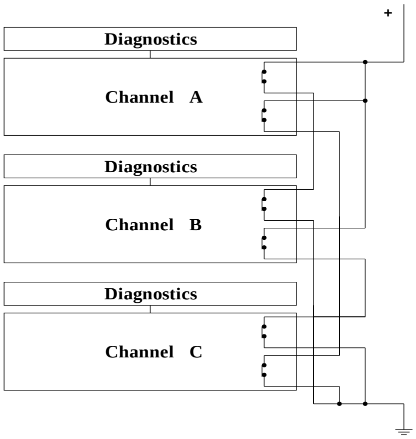


Fig. 3.11 2oo3 electrical diagram

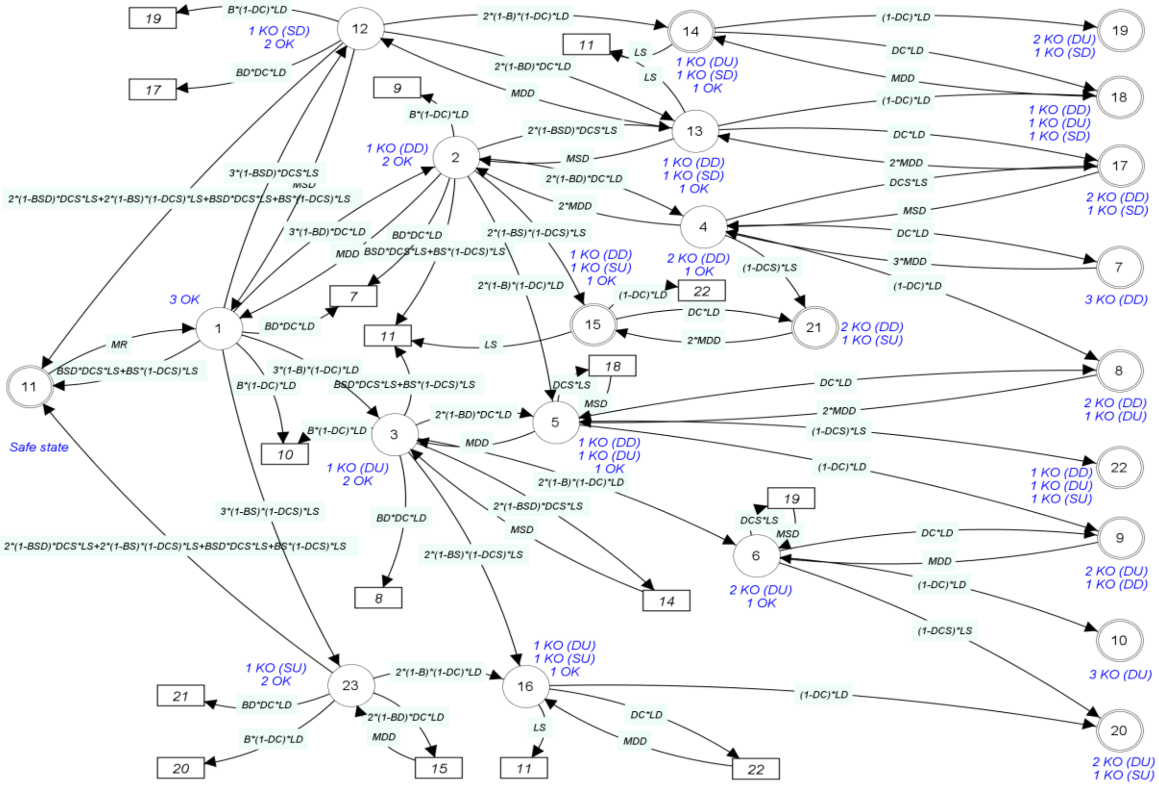


Fig. 3.12 2oo3 multi-phase Markov model

3.1.2 Results presentation and discussion

The obtained results are summarized in the following two tables:

Table 3.2 Modeling results for the PFD_{avg}

Approaches	**With safe failures**						**Without safe failures**					
DC= DCS	$\lambda_D = 2.5E-7$ h^{-1} $\lambda_S = 2.5E-5$ h^{-1}			$\lambda_D = 2.5E-5$ h^{-1} $\lambda_S = 2.5E-7$ h^{-1}			$\lambda_D = 2.5E-7$ h^{-1}			$\lambda_D = 2.5E-5$ h^{-1}		
	$\beta = 2\%$ $\beta_S = 20\%$	$\beta = 10\%$ $\beta_S = 10\%$	$\beta = 20\%$ $\beta_S = 2\%$	$\beta = 2\%$ $\beta_S = 20\%$	$\beta = 10\%$ $\beta_S = 10\%$	$\beta = 20\%$ $\beta_S = 2\%$	$\beta = 2\%$	$\beta = 10\%$	$\beta = 20\%$	$\beta = 2\%$	$\beta = 10\%$	$\beta = 20\%$
1oo1												
0 %	1.0952E-3			0.102			1.0958E-3			0.102		
60 %	4.3947E-4			4.2716E-2			4.3973E-4			4.2717E-2		
90 %	1.1139E-4			1.1062E-2			1.1146E-4			1.1063E-2		
1oo2												
0 %	2.3345E-5	1.1067E-4	2.1984E-4	1.5259E-2	2.1894E-2	3.0293E-2	2.3451E-5	1.1087E-4	2.2015E-4	1.5266E-2	2.1900E-2	3.0298E-2
60 %	8.9963E-6	4.4008E-5	8.7772E-5	3.1877E-3	6.3214E-3	1.0259E-2	9.0193E-6	4.4070E-5	8.7885E-5	3.1890E-3	6.3224E-3	1.0260E-2
90 %	2.2131E-6	1.1003E-5	2.1990E-5	3.7480E-4	1.2299E-3	2.3002E-3	2.2164E-6	1.1016E-5	2.2017E-5	3.7489E-4	1.2300E-3	2.3002E-3
2oo2												
0 %	2.0582E-3	1.9683E-3	1.8636E-3	0.1887	0.1821	0.1737	2.1682E-3	2.0807E-3	1.9715E-3	0.1888	0.1822	0.1738
60 %	8.5169E-4	8.1614E-4	7.7302E-4	8.2223E-2	7.9088E-2	7.5152E-2	8.7041E-4	8.3536E-4	7.9154E-4	8.2241E-2	7.9107E-2	7.5170E-2
90 %	2.1942E-4	2.1059E-4	1.9964E-4	2.1748E-2	2.0893E-2	1.9823E-2	2.2069E-4	2.1189E-4	2.0089E-4	2.1759E-2	2.0894E-2	1.9824E-2
1oo2D												
0 %	2.3345E-5	1.1067E-4	2.1984E-4	1.5259E-2	2.1894E-2	3.0293E-2	2.3451E-5	1.1087E-4	2.2015E-4	1.5266E-2	2.1900E-2	3.0298E-2
60 %	9.1018E-6	4.4096E-5	8.7840E-5	3.1880E-3	6.3192E-3	1.0254E-2	9.0133E-6	4.4040E-5	8.7825E-5	3.1884E-3	6.3197E-3	1.0254E-2
90 %	2.2446E-6	1.1001E-5	2.1947E-5	3.7400E-4	1.2255E-3	2.2913E-3	2.2074E-6	1.0971E-5	2.1927E-5	3.7398E-4	1.2255E-3	2.2914E-3
1oo3												
0 %	2.1879E-5	1.0937E-4	2.1869E-4	4.0986E-3	1.2359E-2	2.2635E-2	2.1913E-5	1.0955E-4	2.1908E-4	4.1008E-3	1.2361E-2	2.2637E-2
60 %	8.7543E-6	4.3766E-5	8.7524E-5	1.0190E-3	4.4800E-3	8.7905E-3	8.7686E-6	4.3841E-5	8.7680E-5	1.0192E-3	4.4802E-3	8.7907E-3
90 %	2.1935E-6	1.0967E-5	2.1932E-5	2.2204E-4	1.0991E-3	2.1940E-3	2.1971E-6	1.0986E-5	2.1971E-5	2.2205E-4	1.0991E-3	2.1941E-3
2oo3												
0 %	2.5951E-5	1.1296E-4	2.2181E-4	3.7550E-2	4.0936E-2	4.5585E-2	2.6525E-5	1.1350E-4	2.2230E-4	3.7596E-2	4.0977E-2	4.5621E-2
60 %	9.4770E-6	4.4481E-5	8.8249E-5	7.5248E-3	1.0004E-2	1.3195E-2	9.5207E-6	4.4526E-5	8.8295E-5	7.5285E-3	1.0007E-2	1.3198E-2
90 %	2.2537E-6	1.1076E-5	2.2105E-5	6.8051E-4	1.4917E-3	2.5125E-3	2.2549E-6	1.1078E-5	2.2108E-5	6.8058E-4	1.4918E-3	2.5126E-3

Table 3.3 Modeling results for the *PFH*

Approaches	**With safe failures**						**Without safe failures**					
DC*= *DCS	$\lambda_D = 2.5E - 7$ h^{-1} $\lambda_S = 2.5E - 5$ h^{-1}			$\lambda_D = 2.5E - 5$ h^{-1} $\lambda_S = 2.5E - 7$ h^{-1}			$\lambda_D = 2.5E - 7$ h^{-1}			$\lambda_D = 2.5E - 5$ h^{-1}		
	$\beta = 2\%$ $\beta_S = 20\%$	$\beta = 10\%$ $\beta_S = 10\%$	$\beta = 20\%$ $\beta_S = 2\%$	$\beta = 2\%$ $\beta_S = 20\%$	$\beta = 10\%$ $\beta_S = 10\%$	$\beta = 20\%$ $\beta_S = 2\%$	$\beta = 2\%$	$\beta = 10\%$	$\beta = 20\%$	$\beta = 2\%$	$\beta = 10\%$	$\beta = 20\%$
1oo1												
0 %	2.4958E-7			2.2449E-5			2.4973E-7			2.2449E-5		
60 %	2.4974E-7			2.3932E-5			2.4989E-7			2.3932E-5		
90 %	2.4982E-7			2.4723E-5			2.4997E-7			2.4723E-5		
1oo2												
0 %	5.4831E-9	2.5381E-8	5.0255E-8	4.7416E-6	6.0492E-6	7.7163E-6	5.5253E-9	2.5440E-8	5.0339E-8	4.7444E-6	6.0517E-6	7.7183E-6
60 %	3.6935E-9	1.7650E-8	3.5096E-8	2.2961E-6	3.4300E-6	4.8586E-6	3.7123E-9	1.7683E-8	3.5148E-8	2.2975E-6	3.4312E-6	4.8597E-6
90 %	2.7972E-9	1.3778E-8	2.7504E-8	8.0300E-7	1.8375E-6	3.1333E-6	2.8040E-9	1.3797E-8	2.7539E-8	8.0338E-7	1.8379E-6	3.1336E-6
2oo2												
0 %	4.5812E-7	4.3752E-7	4.1417E-7	4.0124E-5	3.8815E-5	3.7149E-5	4.9393E-7	4.7401E-7	4.4911E-7	4.0154E-5	3.886E-5	3.7180E-5
60 %	4.80055E-7	4.6574E-7	4.4825E-7	4.5552E-5	4.4417E-5	4.2988E-5	4.9606E-7	4.8210E-7	4.6463E-7	4.5567E-5	4.4433E-5	4.3005E-5
90 %	4.9303E-7	4.8168E-7	4.6785E-7	4.8639E-5	4.7604E-5	4.6309E-5	4.9714E-7	4.8615E-7	4.7241E-7	4.8644E-5	4.7609E-5	4.6313E-5
1oo2D												
0 %	5.4831E-9	2.5381E-8	5.0255E-8	4.7416E-6	6.0492E-6	7.7163E-6	5.5253E-9	2.5440E-8	5.0339E-8	4.7444E-6	6.0517E-6	7.7183E-6
60 %	1.4717E-8	2.1670E-8	3.0361E-8	2.1661E-6	2.7459E-6	3.4767E-6	2.2131E-9	1.0189E-8	2.0160E-8	2.1548E-6	2.7356E-6	3.4676E-6
90 %	5.3515E-9	6.9553E-9	8.9599E-9	5.7937E-7	7.3226E-7	9.2377E-7	5.5363E-10	2.5488E-9	5.0429E-9	5.7469E-7	7.2797E-7	9.1998E-7
1oo3												
0 %	4.9931E-9	2.4956E-8	4.9901E-8	1.3174E-6	3.1120E-6	5.3457E-6	5.0010E-9	2.4998E-8	4.9990E-8	1.3186E-6	3.1130E-6	5.3465E-6
60 %	3.4944E-9	1.7469E-8	3.4935E-8	5.0985E-7	1.8704E-6	3.5638E-6	3.5002E-9	1.7499E-8	3.4997E-8	5.1010E-7	1.8707E-6	3.5640E-6
90 %	2.7454E-9	1.3726E-8	2.7450E-8	2.8625E-7	1.3827E-6	2.7510E-6	2.7500E-9	1.3750E-8	2.7499E-8	2.8628E-7	1.3828E-6	2.7511E-6
2oo3												
0 %	6.3231E-9	2.6095E-8	5.0841E-8	1.1577E-5	1.1912E-5	1.2447E-5	6.5740E-9	2.6325E-8	5.1038E-8	1.1596E-5	1.1929E-5	1.2462E-5
60 %	4.0892E-9	1.8006E-8	3.5410E-8	5.8683E-6	6.5484E-6	7.4477E-6	4.1366E-9	1.8051E-8	3.5451E-8	5.8724E-6	6.5523E-6	7.4511E-6
90 %	2.9078E-9	1.3888E-8	2.7615E-8	1.8373E-6	2.7478E-6	3.8984E-6	2.9120E-9	1.3892E-8	2.2619E-8	1.8376E-6	2.7481E-6	3.8986E-6

It seems from Table 3.2, which gathers the values of *PFD$_{avg}$* obtained from the two versions of the multi-phase Markov models, that even the important variation of the values of all of the failure rates, diagnostic coverage and β factors does not significantly make a difference between taking and eliminating the safe failures in the estimation of such metric. This fact is so obvious for the 1oo1, 1oo3 and even for the 1oo2D. For the rest of architectures, the difference is extremely tiny and it could not be considered effective from any perspective. For instance, let us compare the case of $\lambda_D = 2.5E-7\ h^{-1}, \lambda_S = 2.5E-5\ h^{-1}, DC = 60\%, \beta = 2\%$ and $\beta_S = 20\%$ and the one of $\lambda_D = 2.5E-7\ h^{-1}, DC = 60\%$ and $\beta = 2\%$ for the 2oo2 architecture, since they form one of the biggest differences in the whole table. The relative variation (i.e., $\Delta v/v$) between these two cases is 2.15E-2. Furthermore, their visual presentation is provided in Fig. 3.13 (a).

Concerning Table 3.3, which rounds up the values of *PFH*, the general situation could be considered similar to the preceding one. The only exception is the case of 1oo2D architecture, where the difference between taking and eliminating the contribution of the safe failures could be judged significant especially for the cases where $DC > 0$. Actually, this matter is expected for this specific architecture, since it is well known that the occurrence of a detected safe failure and an undetected dangerous failure can disable the safety function, the fact that it sounds that it has no big effects on the estimation of *PFD$_{avg}$*. As shows Fig. 3.13 (b) that compares the case of $\lambda_D = 2.5E-7\ h^{-1}, \lambda_S = 2.5E-5\ h^{-1}, DC = 90\%, \beta = 2\%$ and $\beta_S = 20\%$, and the one of $\lambda_D = 2.5E-7\ h^{-1}, DC = 90\%$ and $\beta = 2\%$ for the 1oo2D, removing the safe failures is leading to underestimation in the *PFH* value, which is not the case with the other treated architectures.

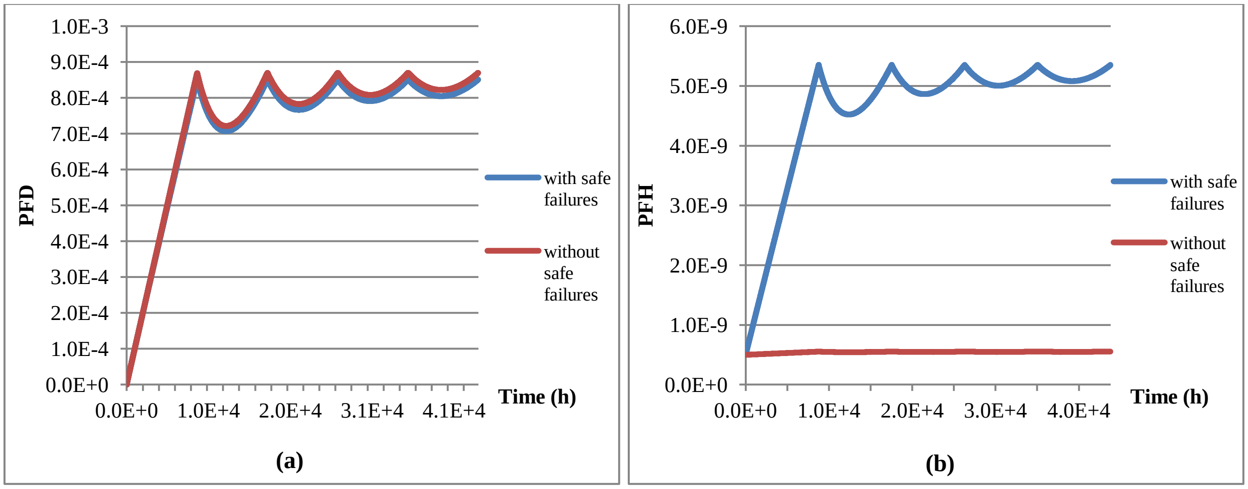


Fig. 3.13 Impact of safe failures on the safety integrity represented by: (a) *PFD* for 2oo2 and (b) *PFH* for 1oo2D

3.2 Quantitative evaluation of dangerous failures' impact on the operational integrity

Besides the intended safety functions, it is very important also to ensure that the SIS is not causing the loss of production through the nuisance trips and the spurious activations of the safety functions. This aspect is commonly known as *operational integrity* or even *production integrity* and it is usually measured by means of the *average probability of failing safely* (*PFS_{avg}*), the *spurious trip rate* (*STR*) and also the *mean time to failure-spurious* (*$MTTF_{spurious}$*). According to (ISA-TR84.00.02-2002, 2002), *PFS* is "*a value that looks at all failures and indicates the probability of those failures that are in a safe mode"* and *$MTTF_{spurious}$* is "*the mean time to a failure of the SIS which results in a spurious or false trip of the process or equipment under control (EUC)".* The *STR* is defined in (PDS, 2010) as "*the mean number of spurious activations of the safety system per time unit*.

In purpose of simplifying the estimation of the operational integrity metrics it is preferable to neglect the contribution of the dangerous failures (for some configurations). The main objective of this section is to investigate the impotence of ignoring those failures in the estimation of *PFS_{avg}* and *STR* by quantitatively compare the values of these two performance indicators that are obtained from two versions of multi-phase Markov models. In the first version, the dangerous failures are considered, where in the second one they are excluded.

To achieve this purpose, we can keep using the Markov models that have been employed in the previous section by just specifying and considering the states in which the system has failed safely (i.e., shutdown of the EUC), and remove all the dangerous failures' contributions for the second version of models. The following table consists of the systems safe failure states in each multi-phase Markov model of each considered configuration. By the way, the values of Table 3.1 will be also considered in this section.

Table 3.4 Safe failure states of each configuration

Architecture	Failure States
1oo1 (Fig. 3.2)	4
1oo2 (Fig. 3.4)	7
2oo2 (Fig. 3.6)	6
1oo2D (Fig. 3.8)	6, 9, 10
1oo3 (Fig. 3.10)	11
2oo3 (Fig. 3.12)	11

3.2.1 Results presentation and discussion

The following two tables contain all the modeling results for the different architectures:

Table 3.5 Modeling results for the PFS_{avg}

Approaches	**With dangerous failures**						**Without dangerous failures**					
DC= DCS	$\lambda_D = 2.5E-7$ h^{-1} $\lambda_S = 2.5E-5$ h^{-1}			$\lambda_D = 2.5E-5$ h^{-1} $\lambda_S = 2.5E-7$ h^{-1}			$\lambda_S = 2.5E-7$ h^{-1}			$\lambda_S = 2.5E-5$ h^{-1}		
	$\beta = 2\%$ $\beta_S = 20\%$	$\beta = 10\%$ $\beta_S = 10\%$	$\beta = 20\%$ $\beta_S = 2\%$	$\beta = 2\%$ $\beta_S = 20\%$	$\beta = 10\%$ $\beta_S = 10\%$	$\beta = 20\%$ $\beta_S = 2\%$	$\beta_S = 20\%$	$\beta_S = 10\%$	$\beta_S = 2\%$	$\beta_S = 20\%$	$\beta_S = 10\%$	$\beta_S = 2\%$
1oo1												
0 %	5.9865E-4			5.3850E-6			5.9967E-6			5.9931E-4		
60 %	5.9904E-4			5.7406E-6			5.9967E-6			5.9931E-4		
90 %	5.9924E-4			5.9304E-6			5.9967E-6			5.9931E-4		
1oo2												
0 %	1.0773E-3	1.1370E-3	1.1847E-3	9.7976E-6	1.0280E-5	1.0671E-5	1.0793E-5	1.1393E-5	1.1873E-5	1.0782E-3	1.1381E-3	1.1859E-3
60 %	1.1137E-3	1.1556E-3	1.1890E-3	1.0711E-5	1.1095E-5	1.1404E-5	1.1154E-5	1.1573E-5	1.1909E-5	1.1141E-3	1.1560E-3	1.1895E-3
90 %	1.1320E-3	1.1649E-3	1.1912E3	1.1215E-5	1.1537E-5	1.1796E-5	1.1334E-5	1.1663E-5	1.1927E-5	1.1321E-3	1.1650E-3	1.1913E-3
2oo2												
0 %	1.8967E-4	1.4729E-4	1.1458E-4	9.7989E-7	4.9916E-7	1.0941E-7	1.2077E-6	6.1030E-7	1.3253E-7	1.9007E-4	1.4759E-4	1.1480E-4
60 %	1.1614E-4	8.0972E-5	5.3249E-5	7.7387E-7	3.9064E-7	8.2338E-8	8.4316E-7	4.2418E-7	8.9042E-8	1.1624E-4	8.1039E-5	5.3292E-5
90 %	7.4723E-5	4.3433E-5	1.8491E-5	6.4623E-7	3.2404E-7	6.5924E-8	6.6059E-7	3.3095E-7	6.7258E-8	7.4739E-5	4.3442E-5	1.8495E-5
1oo2D												
0 %	1.0773E-3	1.1370E-3	1.1849E-3	2.5440E-5	3.0244E-5	3.6143E-5	1.0794E-5	1.1394E-5	1.1873E-5	1.0788E-3	1.1381E-3	1.1859E-3
60 %	4.6740E-4	4.7356E-4	4.7856E-4	1.1120E-5	2.6664E-5	4.6219E-5	4.6774E-6	4.7374E-6	4.7853E-6	4.6755E-4	4.7354E-4	4.7834E-4
90 %	1.6206E-4	1.4132E-4	1.2483E-4	7.4227E-6	2.8983E-5	5.608E-5	1.6191E-6	1.4092E-6	1.2413E-6	1.6202E-4	1.4106E-4	1.2428E-4
1oo3												
0 %	1.5553E-3	1.6747E-3	1.7702E-3	1.4120E-5	1.5134E-5	1.5951E-5	1.5591E-5	1.6790E-5	1.7750E-5	1.5567E-3	1.6763E-3	1.7719E-3
60 %	1.6279E-3	1.7115E3	1.7784E-3	1.5650E-5	1.6435E-5	1.7065E-5	1.6311E-5	1.7150E-5	1.7822E-5	1.6284E-3	1.7121E-3	1.7790E-3
90 %	1.6642E-3	1.7299E-3	1.7825E-3	1.6497E-5	1.7142E-5	1.7661E-5	1.6670E-5	1.7330E-5	1.7858E-5	1.6643E-3	1.7300E-3	1.7826E-3
2oo3												
0 %	3.0934E-4	2.9384E-4	2.8395E-4	1.1747E-6	6.0100E-7	1.4533E-7	1.2245E-6	6.3150E-7	1.5767E-7	3.0972E-4	2.9430E-4	2.8446E-4
60 %	1.7335E-4	1.4938E-4	1.3116E-4	8.4319E-7	4.2771E-7	9.6902E-8	8.5040E-7	4.3298E-7	9.9202E-8	1.7343E-4	1.4947E-4	1.3126E-4
90 %	9.0620E-5	6.2235E-5	3.9758E-5	6.6198E-7	3.3266E-7	6.9597E-8	6.6249E-7	3.3322E-7	6.9843E-8	9.0625E-5	6.2242E-5	3.9764E-5

Table 3.6 Modeling results for the *STR*

Approaches	With dangerous failures						Without dangerous failures					
	$\lambda_D = 2.5E-7$ h^{-1} $\lambda_S = 2.5E-5$ h^{-1}			$\lambda_D = 2.5E-5$ h^{-1} $\lambda_S = 2.5E-7$ h^{-1}			$\lambda_S = 2.5E-7$ h^{-1}			$\lambda_S = 2.5E-5$ h^{-1}		
DC*= *DCS	$\beta =$ 2% $\beta_S =$ 20%	$\beta =$ 10% $\beta_S =$ 10%	$\beta =$ 20% $\beta_S =$ 2%	$\beta =$ 2% $\beta_S =$ 20%	$\beta =$ 10% $\beta_S =$ 10%	$\beta =$ 20% $\beta_S =$ 2%	$\beta_S =$ 20%	$\beta_S =$ 10%	$\beta_S =$ 2%	$\beta_S =$ 20%	$\beta_S =$ 10%	$\beta_S =$ 2%
1oo1												
0 %	2.4958E-5			2.2449E-7			2.4999E-7			2.4985E-5		
60 %	2.4974E-5			2.3932E-7			2.4999E-7			2.4985E-5		
90 %	2.4982E-5			2.4723E-7			2.4999E-7			2.4985E-5		
1oo2												
0 %	4.4910E-5	4.7399E-5	4.9390E-5	4.0844E-7	4.2855E-7	4.4486E-7	4.4999E-7	4.7499E-7	4.9499E-7	4.4951E-5	4.7445E-5	4.94415E-5
60 %	4.6431E-5	4.8175E-5	4.9570E-5	4.4653E-7	4.6253E-7	4.7541E-7	4.6499E-7	4.8249E-7	4.9649E-7	4.6448E-5	4.8194E-5	4.9591E-5
90 %	4.7191E-5	4.8563E-5	4.9660E-5	4.6756E-7	4.8100E-7	4.9177E-7	4.7249E-7	4.8624E-7	4.9724E-7	4.7196E-5	4.8568E-5	4.9666E-5
2oo2												
0 %	7.9087E-6	6.1420E-6	4.7787E-6	4.0847E-8	2.0808E-8	4.5612E-9	5.0350E-8	2.5443E-8	5.5254E-9	7.9252E-6	6.1544E-6	4.7881E-6
60 %	4.8425E-6	3.3765E-6	2.2208E-6	3.2261E-8	1.6285E-8	3.4326E-9	3.5151E-8	1.7684E-8	3.7122E-9	4.8466E-6	3.3793E-6	2.2226E-6
90 %	3.1153E-6	1.8109E-6	7.7115E-7	2.6941E-8	1.3509E-8	2.7483E-9	2.7504E-8	1.3797E-8	2.8040E-9	3.1160E-6	1.8113E-6	7.7131E-7
1oo2D												
0 %	4.4910E-5	4.7399E-5	4.9390E-5	4.0844E-7	4.2855E-7	4.4487E-7	4.4999E-7	4.7499E-7	4.9499E-7	4.4951E-5	4.7446E-5	4.9441E-5
60 %	1.9485E-5	1.9741E-5	1.9948E-5	3.2964E-7	8.8474E-7	1.5829E-6	1.9500E-7	1.9750E-7	1.9950E-7	1.9492E-5	1.9742E-5	1.9942E-5
90 %	6.7563E-6	5.8914E-6	5.2035E-6	2.9537E-7	1.1678E-6	2.2644E-6	6.7500E-8	5.8751E-8	5.1751E-8	6.7548E-6	5.8807E-6	5.1814E-6
1oo3												
0 %	6.4841E-5	6.9817E-5	7.3797E-5	5.8863E-7	6.3088E-7	6.6495E-7	6.4999E-7	6.9999E-7	7.3998E-7	6.4899E-5	6.9883E-5	7.3869E-5
60 %	6.7864E-5	7.1350E-5	7.4139E-5	6.5248E-7	6.8515E-7	7.1140E-7	6.7999E-7	7.1499E-7	7.4299E-7	6.7889E-5	7.1377E-5	7.4168E-5
90 %	6.9378E-5	7.2118E-5	7.4310E-5	6.8761E-7	7.1464E-7	7.3628E-7	6.9499E-7	7.2249E-7	7.4449E-7	6.9384E-5	7.2125E-5	7.4317E-5
2oo3												
0 %	1.2899E-5	1.2254E-5	1.1842E-5	4.8970E-8	2.5055E-8	6.0593E-9	5.1049E-8	2.6327E-8	6.5741E-9	1.2915E-5	1.2273E-5	1.1863E-5
60 %	7.2287E-6	6.2297E-6	5.4703E-6	3.5152E-8	1.7831E-8	4.0401E-9	3.5453E-8	1.8051E-8	4.1361E-9	7.2320E-6	6.2335E-6	5.4745E-6
90 %	3.7784E-6	2.5951E-6	1.6581E-6	2.7598E-8	1.3868E-8	2.9016E-9	2.7619E-8	1.3892E-8	2.9118E-9	3.7786E-6	2.5954E-6	1.6584E-6

Actually, several remarks could be noticed from Table 3.5 that holds the values of PFS_{avg} estimated via multi-phase Markov models for some of the most employed $KooN$ configurations. At the beginning, neglecting the contribution of the dangerous failures is causing the overestimation of the values of this performance indicator for the 1oo1, 1oo2, 1oo3, 2oo3 and also the 2oo2. In most of the cases, this matter does not constitute a shortcoming for the operational integrity and even more it could be viewed advantageous in some applications. Regarding the 1oo2D, eliminating the dangerous failures is considerably affecting the PFS_{avg}, especially when $\lambda_D > \lambda_S$, by reducing its values compared to the ones where such failures are taken into account. The main cause of this underestimation is referred, as illustrates Fig. 3.8, to the ability of the diagnostic devices of this architecture to take the EUC to the safe state once they detect the occurrence of a dangerous failure. Apart from the 1oo2D configuration, Fig. 3.14 (a) demonstrates the discussed conservative trait for the case of $\lambda_D = 2.5E - 5\ h^{-1}, \lambda_S = 2.5E - 7\ h^{-1}$and $DC = 0\%,$ and the case of $\lambda_S = 2.5E - 7\ h^{-1}$and $DC = 0\%,$ for the 1oo1 architecture.

Turning now to the other operational integrity metric (i.e., *STR*), which is addressed in Table 3.6. In a similar fashion to the previous performance indicator, eliminating the dangerous failures leads to increasing the *STR* values for the 1oo1, 1oo2, 2oo2, 1oo3 and 2oo3 configurations. For the 1oo2D, the role of the dangerous detected failure still significant, where the deference between taking and ignoring the dangerous failures' contribution is raising as the value of the *DC* factor increases. This fact could be verified (as shows Fig. 3.14 (b)) through comparing the relative variations (i.e., (STR_{with} - $STR_{without}$)/STR_{with}) of the cases where $\lambda_D = 2.5E - 5\ h^{-1}, \lambda_S = 2.5E - 7\ h^{-1}, \beta = 2\%, \beta_S = 20\%$, and $\lambda_D = \lambda_S = 2.5E - 7\ h^{-1},\ \beta_S = 20\%$ for *DC=60%* on the one hand and *DC=90%* on the other one.

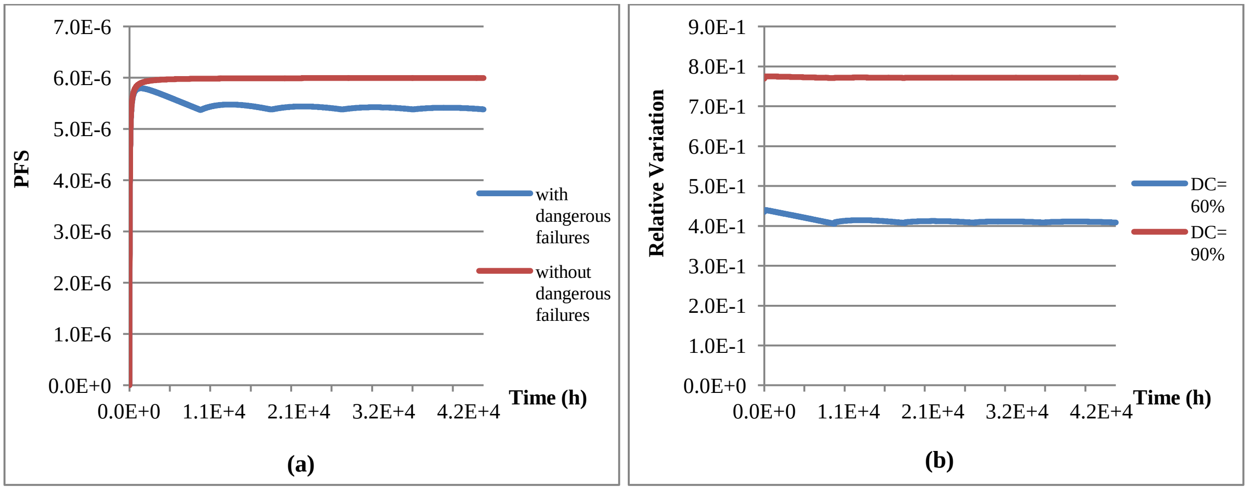


Fig. 3.14 (a) impact of dangerous failures on *PFS* for the 1oo1 and (b) impact of the *DC* value on *STR* for the 1oo2D

3.3 Conclusion

The quantitative comparison between two *PFD_{avg}* and *PFH* values obtained from two different multi-phase Markov models, which represent an appropriate way to model the periodically tested systems, for the configurations 1oo1, 1oo2, 2oo2, 1oo3 and 2oo3 has demonstrated that in spite of the difference between the safe and dangerous failure rates, passing over the safe failures in the estimation of those safety integrity metrics could only lead to slightly elevate their values, the matter that generally does not affect safety in a negative manner. For the 1oo2D architecture, it is well known that the safe detected failure in presence of another dangerous undetected one can cause the loss of the safety function, the reason that makes the proposal of ignoring the safe failures (at least the detected ones) in the calculation of *PFD_{avg}* and *PFH* erroneous and misleading.

When it comes to the elimination of the dangerous failures' contribution in the operational integrity, which is measured in this work by the *PFS_{avg}* and *STR*, the deep assessment that has been performed in the second section employing the same principles and means of the earlier one has confirmed that such practice does not cause any negative effects on the evaluation of this type of performance for all the considered configurations excepting the 1oo2D. Indeed, for all the architectures that allow their diagnostic devices to automatically *de-energize* the outputs when they detect the occurrence of a dangerous failure (including the 1oo2D) the inclusion of the dangerous detected failures in the estimation of the operational integrity related metrics is indisputable.

4. MODELING THE SAFETY INSTRUMENTED SYSTEMS' PERFORMANCE

It is common to consider that the proper way to determine the different performance indicators of SISs is through the usage of the different broadly used and accepted reliability tools like Fault trees, Markov models and Petri nets. Virtually, a good number of engineers are not familiar with such modeling approaches that are relatively difficult and the possibility of making mistakes in the modeling process is always there. Consequently, employing directly the analytical formulas, especially those provided in a normative framework, is generally regarded as a simpler and safer alternative.

As a safety-based standard, the IEC 61508 provides a set of analytical expressions for PFD_{avg} and PFH of some of the commonly used $K$oo$N$ architectures. Additionally, part 2 of the technical report ISA-TR 84.00.02 (ISA-TR84.00.02-2002, 2002) contains a set of PFD_{avg} and STR analytical expressions of several configurations. The Norwegian organization SINTEF suggests simplified equations for PFD_{avg}, PFH and STR in (PDS, 2006; PDS, 2010) of various architectures and also generalized formulation of these indicators, but by neglecting the contribution of dangerous detected failures and the common cause proportion (β) compared to the unity (i.e., β <<1).

Also, PFH generalized formulas are proposed in (Jin, et al., 2013), where the limitation of neglecting the dangerous detected failures is conquered. Moreover, Fault trees and Markov models related to typical architectures are developed and their approximated PFD_{avg} and PFS_{avg} are extracted in (Goble, 2010). What's more, many other valuable contributions have been made regarding this topic such as (Smith, 2007; Innal, 2008; Lundteigen, et al., 2008 (a); Oliveira, 2009; Oliveira, et al., 2010; Torres-Echeverría, et al., 2011).

In this chapter, we provide a new generalization of the different performance indicators' analytical formulas, namely: PFD_{avg} and PFH for the safety integrity, and PFS_{avg} and STR for the operational integrity by focusing on taking the contribution of most of the involved factors into consideration and making those expressions as simple as possible. Accordingly, the user can easily employ them and flexibly treat the different real-world situations by means of the same formulas.

4.1 Safety integrity related metrics

Actually, several cases and scenarios will be treated in this section to provide generalized analytical expressions for the two performance indicators *PFD*$_{avg}$ and *PFH*, that commensurate with the specifications and requirements of each situation.

4.1.1 Considering the dangerous (detected/undetected) failures with proof tests

- ***Estimation of PFD$_{avg}$***

It is well-known that the instantaneous unavailability of a *KooN* system at a given instance *t* can be formulated in the following manner:

$$U_{KooN}(t) = PFD_{KooN}(t) = \sum_{i=N-K+1}^{N} \binom{N}{i} \cdot (q)^i \cdot (1-q)^{N-i} \tag{4.1}$$

where, *q* represents the unavailability of one component at *t*.

As demonstrated in (Innal, 2008), Eq. (4.1) can be simplified as:

$$PFD_{KooN}(t) \approx \binom{N}{N-K+1} \cdot q^{N-K+1} \tag{4.2}$$

In this first case, we will consider the dangerous detected and undetected failures. The unavailability of a component exposed to these two types of failures, as shows Fig. 4.1 could be defined in the following way:

$$\begin{aligned} q &= q_{DD} + q_{DU} - (q_{DD} \cdot q_{DU}) \\ &\approx q_{DD} + q_{DU} \end{aligned} \tag{4.3}$$

where, q_{DD} is the unavailability of a component due to the occurrence of a dangerous detected failure and q_{DU} represents the unavailability that is resulted from a dangerous undetected failure, and they can be calculated as follows:

$$q_{DD} = \frac{\lambda_{DD}}{\lambda_{DD} + \mu_{DD}} (1 - e^{-(\lambda_{DD} + \mu_{DD})t}) \tag{4.4}$$

$$q_{DU} = 1 - e^{-\lambda_{DU} \cdot t} \tag{4.5}$$

where: $\lambda_{DD} = DC \cdot \lambda_D, \lambda_{DU} = (1-DC) \cdot \lambda_D$ and $\mu_{DD} = \dfrac{1}{MTTR}$.

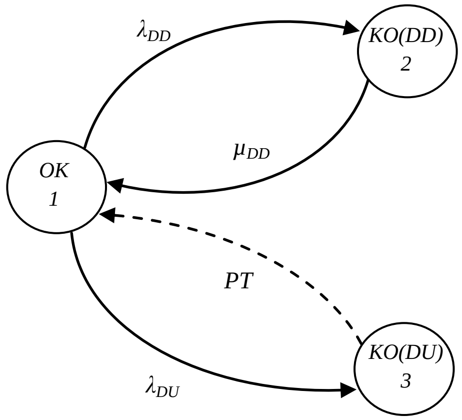


Fig. 4.1 Markov model of a component subject to DD/DU failures and PT

Supposing that the q_{DD} is constant[2] and $\lambda \cdot t << 1$, we can write:

$$q_{DD} \approx \frac{\lambda_{DD}}{\lambda_{DD} + \mu_{DD}} \tag{4.6}$$

$$q_{DU} \approx \lambda_{DU} \cdot t \tag{4.7}$$

By inserting Eqs. (4.6), (4.7) in Eq. (4.3), and this latter in Eq. (4.2) we obtain:

$$PFD_{KooN}(t) \approx \binom{N}{N-K+1} \cdot (\frac{\lambda_{DD}}{\lambda_{DD} + \mu_{DD}} + \lambda_{DU} \cdot t)^{N-K+1} \tag{4.8}$$

The corresponding PFD_{KooN}^{avg} over the interval T_1 can be defined as:

$$PFD_{KooN}^{avg} \approx \frac{\binom{N}{N-K+1}}{T_1} \cdot \int_0^{T_1} (\frac{\lambda_{DD}}{\lambda_{DD} + \mu_{DD}} + \lambda_{DU} \cdot t)^{N-K+1} dt \tag{4.9}$$

Furthermore, Eq. (4.9) can be formulated as:

$$PFD_{KooN}^{avg} \approx \frac{\binom{N}{N-K+1}}{T_1} \cdot \left(\frac{\left(\frac{\lambda_{DD}}{\lambda_{DD} + \mu_{DD}} + \lambda_{DU} \cdot T_1 \right)^{N-K+2} - \left(\frac{\lambda_{DD}}{\lambda_{DD} + \mu_{DD}} \right)^{N-K+2}}{\lambda_{DU} \cdot (N-K+2)} \right) \tag{4.10}$$

[2] This assumption could be inadmissible, since it can lead to underestimating the final results of *PFD*$_{avg}$ and *PFH*. However, as will see later, that underestimation don't appear in the usual cases and even in the extreme cases it appears with a certain amount that can't cause any negative effects on the safety integrity.

It is worth noticing that to further simplify Eq. (4.10) and all the equations that contain the terms $\frac{\lambda_{DD}}{\lambda_{DD}+\mu_{DD}}$, $\frac{\lambda_{DD}^{ind}}{\lambda_{DD}^{ind}+\mu_{DD}}$ and $\frac{\lambda_{DD}^{CCF}}{\lambda_{DD}^{CCF}+\mu_{DD}}$, we can substitute those terms with $\lambda_{DD}\cdot MTTR$, $\lambda_{DD}^{ind}\cdot MTTR$ and $\lambda_{DD}^{CCF}\cdot MTTR$ respectively.

However, to include the CCF events, we know that:

$$PFD_{KooN} \approx PFD_{KooN}^{ind} + PFD_{KooN}^{CCF} \tag{4.11}$$

The two summands of Eq. (4.11) in this case are:

$$PFD_{KooN}^{ind} \approx \frac{\binom{N}{N-K+1}}{T_1}\cdot\left(\frac{\left(\frac{\lambda_{DD}^{ind}}{\lambda_{DD}^{ind}+\mu_{DD}}+\lambda_{DU}^{ind}\cdot T_1\right)^{N-K+2}-\left(\frac{\lambda_{DD}^{ind}}{\lambda_{DD}^{ind}+\mu_{DD}}\right)^{N-K+2}}{\lambda_{DU}^{ind}\cdot\left(N-K+2\right)}\right) \tag{4.12}$$

$$PFD_{KooN}^{CCF} \approx \frac{\left(\frac{\lambda_{DD}^{CCF}}{\lambda_{DD}^{CCF}+\mu_{DD}}+\lambda_{DU}^{CCF}\cdot T_1\right)^{2}-\left(\frac{\lambda_{DD}^{CCF}}{\lambda_{DD}^{CCF}+\mu_{DD}}\right)^{2}}{2\cdot\lambda_{DU}^{CCF}\cdot T_1} \approx \frac{\lambda_{DD}^{CCF}}{\lambda_{DD}^{CCF}+\mu_{DD}}+\frac{\lambda_{DU}^{CCF}\cdot T_1}{2} \tag{4.13}$$

where: $\lambda_{DD}^{ind}=(1-\beta_D)\cdot\lambda_{DD}$, $\lambda_{DU}^{ind}=(1-\beta)\cdot\lambda_{DU}$, $\lambda_{DD}^{CCF}=\beta_D\cdot\lambda_{DD}$ and $\lambda_{DU}^{CCF}=\beta\cdot\lambda_{DU}$.

Finally, we get:

$$\begin{aligned} PFD_{KooN} \approx {} & \frac{\binom{N}{N-K+1}}{T_1}\cdot\left(\frac{\left(\frac{\lambda_{DD}^{ind}}{\lambda_{DD}^{ind}+\mu_{DD}}+\lambda_{DU}^{ind}\cdot T_1\right)^{N-K+2}-\left(\frac{\lambda_{DD}^{ind}}{\lambda_{DD}^{ind}+\mu_{DD}}\right)^{N-K+2}}{\lambda_{DU}^{ind}\cdot\left(N-K+2\right)}\right)+ \\ & \frac{\lambda_{DD}^{CCF}}{\lambda_{DD}^{CCF}+\mu_{DD}}+\frac{\lambda_{DU}^{CCF}\cdot T_1}{2} \end{aligned} \tag{4.14}$$

- ***Estimation of PFH***

To estimate this performance indicator that is mainly used for high and continuous demand modes, we can employ the following formula:

$$PFH_{KooN}(t)=\sum_i w_i(t)\cdot I_{Bi}(t) \tag{4.15}$$

where: $w_i(t)$ denotes the failure frequency of the component *i*, and its formula is given in Eq. (4.16), while $I_{Bi}(t)$ represents the component's Birnbaum importance factor (Birnbaum, 1969), which in turn stands for the conditional probability that, given that *i* has failed, the system is failed and *i* is critical (Dutuit, et al., 2005). This latter can be extracted from the general *PFD*$_{avg}$ as shows Eq. (4.17).

$$w_i(t) = \lambda_i \cdot (1-q) \approx \lambda_i \tag{4.16}$$

$$I_{Bi}(t) = PFD_{Koo(N-1)}(t) \tag{4.17}$$

By assembling Eqs. (4.17), (4.16) and (4.15) and by adding the fact that the channels of a *KooN* system are identical, we can express the average *PFH*$_{KooN}$ in the following format:

$$PFH_{KooN} \approx N \cdot \lambda \cdot PFD_{Koo(N-1)}^{avg} \tag{4.18}$$

In this first case, we have:

$$\begin{aligned} PFH_{KooN} &\approx N \cdot (\lambda_{DD} + \lambda_{DU}) \cdot PFD_{Koo(N-1)}^{avg} \\ &\approx \frac{N \cdot \lambda_D \binom{N-1}{N-K}}{T_1} \cdot \left(\frac{\left(\frac{\lambda_{DD}}{\lambda_{DD} + \mu_{DD}} + \lambda_{DU} \cdot T_1 \right)^{N-K+1} - \left(\frac{\lambda_{DD}}{\lambda_{DD} + \mu_{DD}} \right)^{N-K+1}}{\lambda_{DU} \cdot (N-K+1)} \right) \end{aligned} \tag{4.19}$$

To take the CCF events into account, we have:

$$PFH_{KooN} \approx PFH_{KooN}^{ind} + PFH_{KooN}^{CCF} \tag{4.20}$$

Consequently:

$$\begin{aligned} PFH_{KooN} &\approx \frac{N \cdot \lambda_D^{ind} \binom{N-1}{N-K}}{T_1} \cdot \left(\frac{\left(\frac{\lambda_{DD}^{ind}}{\lambda_{DD}^{ind} + \mu_{DD}} + \lambda_{DU} \cdot T_1 \right)^{N-K+1} - \left(\frac{\lambda_{DD}^{ind}}{\lambda_{DD}^{ind} + \mu_{DD}} \right)^{N-K+1}}{\lambda_{DU}^{ind} \cdot (N-K+1)} \right) + \\ &\qquad \lambda_D^{CCF} \end{aligned} \tag{4.21}$$

where: $\lambda_D^{ind} = \lambda_{DD}^{ind} + \lambda_{DU}^{ind}$ and $\lambda_D^{CCF} = \lambda_{DD}^{CCF} + \lambda_{DU}^{CCF}$.

- ***Validation***

Indeed, the validation of the obtained expressions necessitates comparing their results to the ones obtained from the accepted approaches. The following two tables gather *PFD*$_{avg}$ and *PFH* values of some of the famous architecture obtained from our proposed expressions and form the corresponding multi-phase Markov models (MPM), which can be found in Chapter 3. Actually, to make the comparison more efficient, it is important to carry it out with and without taking the CCF events into consideration.

Table 4.1 *PFD*$_{avg}$ and *PFH* values with DD/DU failures and PT (without CCF)

<table>
<tr><th colspan="5">λ_D=2.5E-6/h, T_1 =8760 h, $MTTR$=8 h and DC=0.6</th></tr>
<tr><th></th><th><b>PFD_{avg} (Eq.(4.10))</b></th><th><b>PFD_{avg} (MPM)</b></th><th><b>PFH(Eq.(4.19))</b></th><th><b>PFH(MPM)</b></th></tr>
<tr><td><b>1oo1</b></td><td>4.3920E-3</td><td>4.3857E-3</td><td>2.5000E-6</td><td>2.4890E-6</td></tr>
<tr><td><b>1oo2</b></td><td>2.5684E-5</td><td>2.5544E-5</td><td>2.1960E-8</td><td>2.1800E-8</td></tr>
<tr><td><b>2oo2</b></td><td>8.7840E-3</td><td>8.7454E-3</td><td>5.0000E-6</td><td>4.9563E-6</td></tr>
<tr><td><b>1oo3</b></td><td>1.6898E-7</td><td>1.6737E-7</td><td>1.9263E-10</td><td>1.9032E-10</td></tr>
<tr><td><b>2oo3</b></td><td>7.7053E-5</td><td>7.6297E-5</td><td>6.5880E-8</td><td>6.5019E-8</td></tr>
</table>

Table 4.2 *PFD*$_{avg}$ and *PFH* values with DD/DU failures and PT (with CCF)

<table>
<tr><th colspan="5">λ_D=2.5E-6/h, T_1 =8760 h, $MTTR$=8 h, DC=0.6, β=0.2 and β_D=0.1</th></tr>
<tr><th></th><th><b>PFD_{avg} (Eq.(4.14))</b></th><th><b>PFD_{avg} (MPM)</b></th><th><b>PFH (Eq.(4.21))</b></th><th><b>PFH (MPM)</b></th></tr>
<tr><td><b>1oo1</b></td><td>4.3920E-3</td><td>4.3857E-3</td><td>2.5000E-6</td><td>2.4890E-6</td></tr>
<tr><td><b>1oo2</b></td><td>8.9365E-4</td><td>8.9307E-4</td><td>3.6511E-7</td><td>3.6470E-7</td></tr>
<tr><td><b>2oo2</b></td><td>7.9068E-3</td><td>7.8779E-3</td><td>4.6500E-6</td><td>4.6134E-6</td></tr>
<tr><td><b>1oo3</b></td><td>8.7729E-4</td><td>8.7637E-4</td><td>3.5011E-7</td><td>3.4980E-7</td></tr>
<tr><td><b>2oo3</b></td><td>9.2654E-4</td><td>9.2646E-4</td><td>3.9534E-7</td><td>3.9451E-7</td></tr>
</table>

Tables 4.1 and 4.2 corroborate the fact that all the *PFD*$_{avg}$ and *PFH* values obtained via the proposed equations for the various configurations are very close to the ones obtained from the multi-phase Markov models with a certain overestimation that is extremely tiny. Obviously, there are no negative effects of assuming that q_{DD} is constant and even by excessively varying the various involved parameters the effects could not be judged significant.

4.1.2 Considering the dangerous undetected failures with proof and partial stroking tests

- ***Estimation of PFD$_{avg}$***

For this case, the dangerous undetected failure rate of each element is split into two parts according to the PST coverage factor θ:

✓ $\lambda_{PT} = (1-\theta) \cdot \lambda_{DU}$, which represents the proportion of failures detected by proof tests;

- ✓ $\lambda_{ST} = \theta \cdot \lambda_{DU}$, which represents the proportion of failures detected by both proof testing and partial stroke testing.

Under these conditions, the unavailability of one component is (see Fig. 4.2):

$$\begin{aligned} q &\approx q_{PT} + q_{ST} \\ &\approx 1 - e^{-\lambda_{PT} \cdot t_{PT}} + 1 - e^{-\lambda_{ST} \cdot t_{ST}} \\ &\approx \quad \lambda_{PT} \cdot t_{PT} + \lambda_{ST} \cdot t_{ST} \end{aligned} \tag{4.22}$$

where, t_{PT} and t_{ST} can be written in function of t, proof tests interval (T_1) and PST interval (T_{ST}):

$$t_{PT} = [t - E(\frac{t}{T_1}) \cdot T_1]$$

$$t_{ST} = [t - E(\frac{t}{T_{ST}}) \cdot T_{ST}]$$

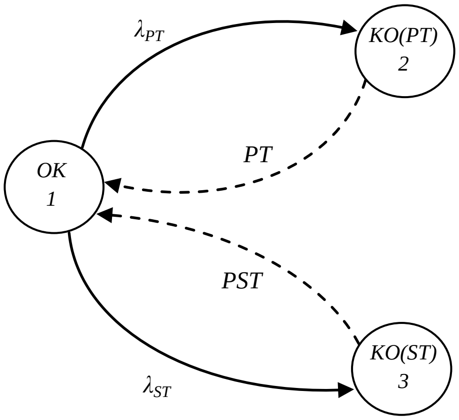


Fig. 4.2 Markov model of a component subject to DU failures, partial and proof tests

We can utilize Eq. (4.2) in this case to get:

$$PFD_{KooN}(t) \approx \begin{pmatrix} N \\ N-K+1 \end{pmatrix} \cdot (\lambda_{PT} \cdot t_{PT} + \lambda_{ST} \cdot t_{ST})^{N-K+1} \tag{4.23}$$

Thus:

$$PFD_{KooN}^{avg} \approx \frac{\begin{pmatrix} N \\ N-K+1 \end{pmatrix}}{T_1} \cdot \int_0^{T_1} (\lambda_{PT} \cdot t_{PT} + \lambda_{ST} \cdot t_{ST})^{N-K+1} dt \tag{4.24}$$

Assuming that PST is performed periodically with a frequency of *m* times in T_1 (i.e., $T_1 = m \cdot T_{ST}$), we can write:

$$PFD_{KooN}^{avg} \approx \frac{\begin{pmatrix} N \\ N-K+1 \end{pmatrix}}{m \cdot T_{ST}} \int_{0}^{m \cdot T_{ST}} (\lambda_{PT} \cdot t_{PT} + \lambda_{ST} \cdot t_{ST})^{N-K+1} dt \tag{4.25}$$

The integral in this latter equation can be rewritten as follows:

$$PFD_{KooN}^{avg} \approx \frac{\begin{pmatrix} N \\ N-K+1 \end{pmatrix}}{m \cdot T_{ST}} \sum_{j=0}^{m-1} \int_{j \cdot T_{ST}}^{(j+1) \cdot T_{ST}} (\lambda_{PT} \cdot t_{PT} + \lambda_{ST} \cdot t_{ST})^{N-K+1} dt \tag{4.26}$$

Furthermore, we can write:

$$\begin{aligned} PFD_{KooN}^{avg} &\approx \frac{\begin{pmatrix} N \\ N-K+1 \end{pmatrix}}{m \cdot T_{ST}} \sum_{j=0}^{m-1} \int_{0}^{T_{ST}} (\lambda_{PT} \cdot (t + j \cdot T_{ST}) + \lambda_{ST} \cdot t)^{N-K+1} dt \\ &\approx \frac{\begin{pmatrix} N \\ N-K+1 \end{pmatrix}}{m \cdot T_{ST}} \sum_{j=0}^{m-1} \int_{0}^{T_{ST}} (\lambda_{PT} \cdot j \cdot T_{ST} + (\lambda_{PT} + \lambda_{ST}) \cdot t)^{N-K+1} dt \\ &\approx \frac{\begin{pmatrix} N \\ N-K+1 \end{pmatrix}}{m \cdot T_{ST}} \sum_{j=0}^{m-1} \int_{0}^{T_{ST}} (\lambda_{PT} \cdot j \cdot T_{ST} + \lambda_{DU} \cdot t)^{N-K+1} dt \end{aligned} \tag{4.27}$$

This last equation can be expressed in the subsequent way:

$$PFD_{KooN}^{avg} \approx \frac{\begin{pmatrix} N \\ N-K+1 \end{pmatrix}}{m \cdot T_{ST}} \sum_{j=0}^{m-1} \frac{((\lambda_{DU} + \lambda_{PT} \cdot j) T_{ST})^{N-K+2} - (\lambda_{PT} \cdot j \cdot T_{ST})^{N-K+2}}{\lambda_{DU} \cdot (N-K+2)} \tag{4.28}$$

In purpose of taking into account the CCFs, we can write:

$$PFD_{KooN}^{ind} \approx \sum_{j=0}^{m-1} \frac{\begin{pmatrix} N \\ N-K+1 \end{pmatrix} \cdot \left[\left(\left(\lambda_{DU}^{ind} + \lambda_{PT}^{ind} \cdot j \right) \cdot T_{ST} \right)^{N-K+2} - \left(\lambda_{PT}^{ind} \cdot j \cdot T_{ST} \right)^{N-K+2} \right]}{\lambda_{DU}^{ind} \cdot (N-K+2) \cdot m \cdot T_{ST}} \tag{4.29}$$

$$PFD_{KooN}^{CCF} \approx \sum_{j=0}^{m-1} \frac{\left(\left(\lambda_{DU}^{CCF} + \lambda_{PT}^{CCF} \cdot j\right) \cdot T_{ST}\right)^2 - \left(\lambda_{PT}^{CCF} \cdot j \cdot T_{ST}\right)^2}{2 \cdot \lambda_{DU}^{CCF} \cdot m \cdot T_{ST}} \approx \frac{T_{ST}}{2}\left(\lambda_{DU}^{CCF} + \lambda_{PT}^{CCF} \cdot (m-1)\right) \tag{4.30}$$

where: $\lambda_{ST}^{ind} = (1-\beta_{ST}) \cdot \lambda_{ST}$, $\lambda_{PT}^{ind} = (1-\beta_{PT}) \cdot \lambda_{PT}$, $\lambda_{DU}^{ind} = \lambda_{ST}^{ind} + \lambda_{PT}^{ind}$, $\lambda_{ST}^{CCF} = \beta_{ST} \cdot \lambda_{ST}$, $\lambda_{PT}^{CCF} = \beta_{PT} \cdot \lambda_{PT}$ and $\lambda_{DU}^{CCF} = \lambda_{PT}^{CCF} + \lambda_{ST}^{CCF}$.

Finally, we obtain:

$$PFD_{KooN} \approx \sum_{j=0}^{m-1} \frac{\binom{N}{N-K+1} \cdot \left[\left(\left(\lambda_{DU}^{ind} + \lambda_{PT}^{ind} \cdot j\right) \cdot T_{ST}\right)^{N-K+2} - \left(\lambda_{PT}^{ind} \cdot j \cdot T_{ST}\right)^{N-K+2}\right]}{\lambda_{DU}^{ind} \cdot (N-K+2) \cdot m \cdot T_{ST}} + \frac{T_{ST}}{2}\left(\lambda_{DU}^{CCF} + \lambda_{PT}^{CCF} \cdot (m-1)\right) \tag{4.31}$$

- ***Estimation of PFH***

In an analogous way to the previous case, we can adopt Eq. (4.18) for this one:

$$PFH_{KooN} \approx \frac{N \cdot \binom{N-1}{N-K}}{m \cdot T_{ST}} \sum_{j=0}^{m-1} \frac{\left(\left(\lambda_{DU} + \lambda_{PT} \cdot j\right) T_{ST}\right)^{N-K+1} - \left(\lambda_{PT} \cdot j \cdot T_{ST}\right)^{N-K+1}}{(N-K+1)} \tag{4.32}$$

Easily, we can extract the *PFH_{KooN}* expression with the consideration of CCF events:

$$PFH_{KooN} \approx \frac{N \cdot \binom{N-1}{N-K}}{m \cdot T_{ST}} \sum_{j=0}^{m-1} \frac{\left(\left(\lambda_{DU}^{ind} + \lambda_{PT}^{ind} \cdot j\right) T_{ST}\right)^{N-K+1} - \left(\lambda_{PT}^{ind} \cdot j \cdot T_{ST}\right)^{N-K+1}}{(N-K+1)} + \lambda_{DU}^{CCF} \tag{4.33}$$

- ***Validation***

In order to authenticate the constructed PFD_{avg} formulas, we can compare their obtained results to those gotten from the PFD_{avg} formulas that are developed in (Jin, et al., 2014) in addition to the Fault tree approach. When it comes to *PFH* expressions, we compare their results to the ones obtained via the corresponding Fault trees, since we did not find any general equations for this performance indicator that take the PST's contribution into account.

The following two tables hold the PFD_{avg} and *PFH* values of some of commonly used *K*oo*N* architectures without considering the CCF events.

Table 4.3 *PFD_{avg}* values with DU failures, PT and PST (without CCF)

λ_{DU}=2.5E-6/*h*, T_1 =8760 h, *m*=4 and θ=0.6			
	Eq. (4.28)	(Jin, et al., 2014)	**Fault tree**
1oo1	6.0225E-3	6.0225E-3	6.0002E-3
1oo2	4.4763E-5	4.4763E-5	4.4406E-5
2oo2	1.2045E-2	1.2062E-2	1.1956E-2
1oo3	3.7189E-7	3.7189E-7	3.6716E-7
2oo3	1.3429E-4	1.3438E-4	1.3248E-4
3oo3	1.8067E-2	1.8118E-2	1.7868E-2
1oo4	3.3239E-9	3.3239E-9	3.2652E-9
2oo4	1.4875E-6	1.4881E-6	1.4589E-6

Table 4.4 *PFH* values with DU failures, PT and PST (without CCF)

λ_{DU}=2.5E-6/*h*, T_1 =8760 h, *m*=4 and θ=0.6		
	Eq. (4.32)	**Fault tree**
1oo1	2.5000E-6	2.4850E-6
1oo2	3.0112E-8	2.9779E-8
2oo2	5.0000E-6	4.9402E-6
1oo3	3.3573E-10	3.3029E-10
2oo3	9.0337E-8	8.8676E-8
3oo3	7.5000E-6	7.366E-6
1oo4	3.7189E-12	3.6390E-12
2oo4	1.3429E-9	1.3102E-9

The first noticeable matter in Table 4.3 is the considerable matching between the two analytical approaches (i.e., our proposed equation and the one in (Jin, et al., 2014)) for all of the studied configurations. Compared to the Fault trees' results, we can observe that the two analytical equations are a little conservative, while this character is "insignificantly" less intense in the case of Eq. (4.28). In Table 4.4 the conservative character still associated with the analytical approach, the fact that can be considered as an expected impact of the approximations that have been taken to simplify its construction. However, the overestimation is too tiny and it has no negative effects on safety integrity.

In what follows, several *PFD_{avg}* and *PFH* values for the 1oo2 architecture are presented that are gotten through several approaches, employing several PST strategies and by taking the contribution of CCFs into consideration.

Table 4.5 *PFD_{avg}* values with DU failures, PT and PST (with CCF)

1oo2, λ_{DU}=0.8E-6/h, T_1 =8760 h, θ=0.65, β_{ST}=0.05 and β_{PT}=0.1			
PST Strategy	**Eq. (4.31)**	(Jin, et al., 2014)	**Fault tree**
Monthly (m=12)	1.34E-4	1.44E-4	1.34E-4
Quarterly (m=4)	1.54E-4	1.54E-4	1.54E-4
Biannually (m=2)	1.86E-4	1.86E-4	1.86E-4
Without (m=1)	3.64E-4	3.64E-4	3.64E-4

Table 4.6 *PFH* values with DU failures, PT and PST (with CCF)

1oo2, λ_{DU}=0.8E-6/h, T_1 =8760 h, θ=0.65, β_{ST}=0.05 and β_{PT}=0.1		
PST Strategy	**Eq. (4.33)**	**Fault tree**
Monthly (m=12)	5.5915E-8	5.5904E-8
Quarterly (m=4)	5.6454E-8	5.6438E-8
Biannually (m=2)	5.7261E-8	5.7237E-8
Without PST (m=1)[3]	8.4541E-8	8.4481E-8

Regardless the case where the PST is monthly implemented (i.e., *m*=12), the results of the different approaches in Table 4.5 are totally identical, and obviously, the consideration of CCF events has diluted the conservative character that is associated to the analytical formulas. Furthermore, the scrutiny of Table 4.6 confirms the validity of Eq. (4.33) to estimate the *PFH* values with any PST strategy.

4.1.3 Considering the dangerous (detected/undetected) failures with proof and partial stroking tests

- ***Estimation of PFD_{avg}***

At this level, the unavailability of one component is:

$$\begin{aligned} q &\approx q_{DD} + q_{PT} + q_{ST} \\ &\approx \frac{\lambda_{DD}}{\lambda_{DD} + \mu_{DD}} + \lambda_{PT} \cdot t_{PT} + \lambda_{ST} \cdot t_{ST} \end{aligned} \qquad (4.34)$$

Once more, we employ Eq. (4.2) to get:

$$PFD_{KooN}(t) \approx \begin{pmatrix} N \\ N-K+1 \end{pmatrix} \cdot \left(\frac{\lambda_{DD}}{\lambda_{DD} + \mu_{DD}} + \lambda_{PT} \cdot t_{PT} + \lambda_{ST} \cdot t_{ST}\right)^{N-K+1} \qquad (4.35)$$

[3] For this case, it is important to mention that the value of β_{ST} must be modified to be equal to the one of β_{PT}

We follow the same previously used steps to find:

$$PFD_{KooN}^{avg} \approx \frac{\begin{pmatrix} N \\ N-K+1 \end{pmatrix}}{m \cdot T_{ST}} \sum_{j=0}^{m-1} \frac{\left(\frac{\lambda_{DD}}{\lambda_{DD}+\mu_{DD}} + \left(\lambda_{DU}+\lambda_{PT}\cdot j\right) T_{ST} \right)^{N-K+2}}{\lambda_{DU}\cdot\left(N-K+2\right)} - \frac{\left(\frac{\lambda_{DD}}{\lambda_{DD}+\mu_{DD}} + \lambda_{PT}\cdot j \cdot T_{ST} \right)^{N-K+2}}{\lambda_{DU}\cdot\left(N-K+2\right)} \tag{4.36}$$

To include the CCF events, we have:

$$PFD_{KooN}^{ind} \approx \frac{\begin{pmatrix} N \\ N-K+1 \end{pmatrix}}{m \cdot T_{ST}} \sum_{j=0}^{m-1} \frac{\left(\frac{\lambda_{DD}^{ind}}{\lambda_{DD}^{ind}+\mu_{DD}} + \left(\lambda_{DU}^{ind}+\lambda_{PT}^{ind}\cdot j\right) T_{ST} \right)^{N-K+2}}{\lambda_{DU}^{ind}\cdot\left(N-K+2\right)} - \frac{\left(\frac{\lambda_{DD}^{ind}}{\lambda_{DD}^{ind}+\mu_{DD}} + \lambda_{PT}^{ind}\cdot j \cdot T_{ST} \right)^{N-K+2}}{\lambda_{DU}^{ind}\cdot\left(N-K+2\right)} \tag{4.37}$$

$$PFD_{KooN}^{CCF} \approx \frac{\lambda_{DD}^{CCF}}{\lambda_{DD}^{CCF}+\mu_{DD}} + \frac{T_{ST}}{2}\left(\lambda_{DU}^{CCF}+\lambda_{PT}^{CCF}\left(m-1\right)\right) \tag{4.38}$$

Finally, we can conclude that:

$$PFD_{KooN} \approx \frac{\begin{pmatrix} N \\ N-K+1 \end{pmatrix}}{m \cdot T_{ST}} \sum_{j=0}^{m-1} \frac{\left(\frac{\lambda_{DD}^{ind}}{\lambda_{DD}^{ind}+\mu_{DD}} + \left(\lambda_{DU}^{ind}+\lambda_{PT}^{ind}\cdot j\right) T_{ST} \right)^{N-K+2}}{\lambda_{DU}^{ind}\cdot\left(N-K+2\right)} - \frac{\left(\frac{\lambda_{DD}^{ind}}{\lambda_{DD}^{ind}+\mu_{DD}} + \lambda_{PT}^{ind}\cdot j \cdot T_{ST} \right)^{N-K+2}}{\lambda_{DU}^{ind}\cdot\left(N-K+2\right)} + \frac{\lambda_{DD}^{CCF}}{\lambda_{DD}^{CCF}+\mu_{DD}} + \frac{T_{ST}}{2}\left(\lambda_{DU}^{CCF}+\lambda_{PT}^{CCF}\left(m-1\right)\right) \tag{4.39}$$

- ***Estimation of PFH***

Again, we employ Eq. (4.18) in this case to obtain:

$$PFH_{KooN} \approx N \cdot (\lambda_{DD} + \lambda_{PT} + \lambda_{ST}) \cdot PFD^{avg}_{Koo(N-1)}$$

$$\approx \frac{N \cdot \lambda_D \binom{N-1}{N-K}}{m \cdot T_{ST}} \sum_{j=0}^{m-1} \frac{\left(\frac{\lambda_{DD}}{\lambda_{DD} + \mu_{DD}} + (\lambda_{DU} + \lambda_{PT} \cdot j) T_{ST} \right)^{N-K+1}}{\lambda_{DU} \cdot (N-K+1)} -$$

$$\frac{\left(\frac{\lambda_{DD}}{\lambda_{DD} + \mu_{DD}} + \lambda_{PT} \cdot j \cdot T_{ST} \right)^{N-K+1}}{\lambda_{DU} \cdot (N-K+1)} \qquad (4.40)$$

At this stage, we can deduce the PFH_{KooN} formula that takes the CCF events into account:

$$PFH_{KooN} \approx \frac{N \cdot \lambda_D^{ind} \binom{N-1}{N-K}}{m \cdot T_{ST}} \sum_{j=0}^{m-1} \frac{\left(\frac{\lambda_{DD}^{ind}}{\lambda_{DD}^{ind} + \mu_{DD}} + (\lambda_{DU}^{ind} + \lambda_{PT}^{ind} \cdot j) T_{ST} \right)^{N-K+1}}{\lambda_{DU}^{ind} \cdot (N-K+1)} -$$

$$\frac{\left(\frac{\lambda_{DD}^{ind}}{\lambda_{DD}^{ind} + \mu_{DD}} + \lambda_{PT}^{ind} \cdot j \cdot T_{ST} \right)^{N-K+1}}{\lambda_{DU}^{ind} \cdot (N-K+1)} + \lambda_D^{CCF} \qquad (4.41)$$

where for this case: $\lambda_D^{ind} = \lambda_{DD}^{ind} + \lambda_{PT}^{ind} + \lambda_{ST}^{ind}$ and $\lambda_D^{CCF} = \lambda_{DD}^{CCF} + \lambda_{PT}^{CCF} + \lambda_{ST}^{CCF}$.

- ***Validation***

Actually, at this stage we do not need to validate the proposed formulas since they are a combination of the previous two cases. However, we can weigh the suggested Eq. (4.36) for PFD_{avg} against the ones constructed in (Oliveira, 2009) as shows Table 4.7. The last three columns in the table hold the PFD_{avg} values that are provided in Table 3 of (Oliveira, 2009), where: (a) stands for the obtained results from Eq. (23) in that reference, (b) represents the results of Eq. (24) and (c) contains the results of the numerical approach developed in the same document.

Table 4.7 PFD_{avg} values with DD/DU failures, PT and PST (without CCF)

λ_D=2.7E-6/*h*, T_1 =43800 h, T_{ST} =730 h, *MTTR*=24 h, *DC*=0.25 and θ=0.8				
	Eq.(4.36)	**Table 3 of** (Oliveira, 2009)		
		(a)	**(b)**	**(c)**
1oo1	9.48E-3	9.53E-3	9.53E-3	9.42E-3
1oo2	1.16E-4	1.21E-4	1.21E-4	1.15E-4
2oo2	1.89E-2	1.91E-2	1.91E-2	1.87E-2
1oo3	1.60E-6	1.31E-6	1.74E-6	1.57E-6
2oo3	3.49E-4	3.64E-4	3.64E-4	3.41E-4
3oo3	2.84E-2	2.86E-2	2.86E-2	2.79E-2
1oo4	2.36E-8	1.33E-8	2.66E-8	2.29E-8
2oo4	6.41E-6	5.22E-6	6.96E-6	6.21E-6
3oo4	6.97E-4	7.28E-4	7.28E-4	6.76E-4
4oo4	3.79E-2	3.81E-2	3.81E-2	3.70E-2

Although, our suggested equations do not take the *MRT* (for the dangerous undetected failures) into account, we can notice the important matching between the values of Eq. (4.36) and the ones of the other three approaches for all the studied architectures, especially with the values of column (c) (i.e., numerical approach) that is considered as the reference of the comparison. Certainly, the same thing can be found in the case of taking the CCF events into consideration by comparing the results of Eq. (4.41) and the ones in Table 5 of (Oliveira, 2009).

4.2 Operational integrity related metrics

This section is dedicated to evaluate the SIS performance in terms of operational integrity by offering analytical formulas for PFS_{avg} and *STR* that could be used for any *K*oo*N* configuration using more direct approach relying on a generalized approximated Markov model.

4.2.1 Generic Markov model for *K*oo*N* architectures (safe failures)

The following figure represents a generalized Markov model related to safe failures for any *K*oo*N* architecture.

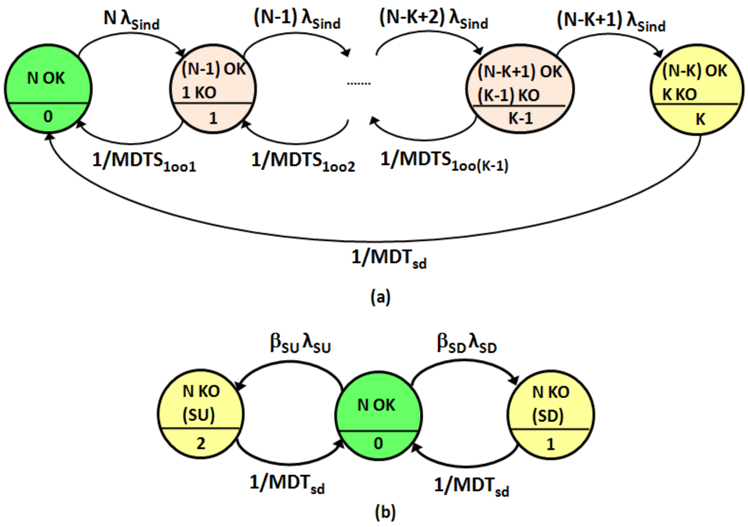


Fig. 4.3 Generic approached Markov model for *K*oo*N* architectures: (a) independent safe failures and (b) dependent safe failures (CCF)

In Fig. 4.3 (a), states numbered from *0* to *K – 1* are operational states, whereas state *K* corresponds to a fail-safe state. As the production is stopped due to a shutdown caused by the spurious activation of the *K*oo*N* system, we assume that the set made up of (SIS + EUC) remains in this state and cannot be further deteriorated. The SIS then needs to be completely repaired and put back in its nominal state so the production can be restarted in the best possible conditions. This assumption originates the transition $1/MDT_{sd}$ (*sd* denotes the shutdown). It can be understood that the safe failure leading to the shutdown state will be immediately brought to light, even if it is a safe undetected one.

The setting of transitions corresponding to the repair of independent safe failures ($1/MDTS_{1ooi}$) can be written as follows:

$$MDTS_{1ooi} = \frac{\lambda_{SUind}}{\lambda_{Sind}} \cdot \left(\frac{T_1}{i+1} + MRT_S \right) + \frac{\lambda_{SDind}}{\lambda_{Sind}} \cdot MTTR_S \tag{4.42}$$

where: $\lambda_{Sind} = \lambda_{SUind+}\ \lambda_{SDind} = (1\text{-}\beta_{SU})\lambda_{SU}+(1\text{-}\beta_{SD})\lambda_{SD}$, MRT_S is the repaire time of a safe undetected failure and $MTTR_S$ of a safe detected failure.

Fig. 4.3 (b) describes the spurious activation of the *K*oo*N* system due to dependent failures. From the fact that these failures are immediately detected and repaired within a mean duration equals $1/MDT_{sd}$, the related Morkov model is exact rather than approximated. This is also true for 1oo*N* configurations, since only one safe failure provokes the sutdown state.

4.2.2 Extracting PFS_{KooN} and STR_{KooN} from the Markov model

PFS_{avg} is the average probability of occupying the shutdown state: state *K* of Fig. 4.3 (a) and states 1 and 2 of Fig. 4.3 (b). The more accurate approach would be deducing these average probabilities from a multi-state Markov model, especially for the state *K*. However, we can give an approximate value of these probabilities by calculating their steady states (asymptotic) values from the proposed approached Markov model:

$$\begin{aligned} PFS_{KooN}^{ind} &\approx p_K(\infty) \approx \frac{N\cdot(N-1)\cdots(N-K+1)\cdot\lambda_{Sind}^{K}}{\frac{1}{MDT_{sd}}\cdot\prod_{i=1}^{K-1}\frac{1}{MDTS_{1ooi}}} \\ &\approx A_N^K\cdot\lambda_{Sind}^K\cdot MDT_{sd}\cdot\prod_{i=1}^{K-1}MDTS_{1ooi} \\ &\approx A_N^K\cdot\lambda_{Sind}\cdot MDT_{sd}\cdot\prod_{i=1}^{K-1}\left(\lambda_{SUind}\cdot\left(\frac{T_1}{i+1}+MRT_S\right)+\lambda_{SDind}\cdot MTTR_S\right) \end{aligned} \quad (4.43)$$

The contribution of CCF events could be given as follows:

$$PFS_{KooN}^{CCF} \approx p_1(\infty)+p_2(\infty)=\left(\beta_{SU}\lambda_{SU}+\beta_{SD}\lambda_{SD}\right)\cdot MDT_{sd} \quad (4.44)$$

The general expression giving the *PFS_{KooN}* can finally be written as:

$$\begin{aligned} PFS_{KooN} = {} & A_N^K\cdot\lambda_{Sind}\cdot MDT_{sd}\cdot\prod_{i=1}^{K-1}\left(\lambda_{SUind}\cdot\left(\frac{T_1}{i+1}+MRT_S\right)+\lambda_{SDind}\cdot MTTR_S\right) \\ & +\left(\beta_{SU}\lambda_{SU}+\beta_{SD}\lambda_{SD}\right)\cdot MDT_{sd} \end{aligned} \quad (4.45)$$

The STR_{KooN}, which represents the average frequency of the *K*oo*N* system spurious activation, can be obtained from the Markov model on the basis of the so-called *critical working states* method (Innal, 2008; Innal, et al., 2010):

$$w_S(0,T)=\sum_{i\in Mc}\Lambda_i\cdot APS_i(0,T)\approx\sum_{i\in Mc}\Lambda_i\cdot p_i(\infty) \quad (4.46)$$

where, $w_S(0,T)$ is the average failure frequency of a given system over the period *T*. M_C denotes the set of the critical working states and Λ_i is the sum of the failure rates starting from the critical working state *i* and finishing in a failed state (shutdown). APS_i characterizes the average probability of sojourn in the critical working state *i* over the same period *T*. Thus, we get:

$$\begin{aligned} STR_{KooN}^{ind} &= p_{K-1}(\infty)\cdot(N-K+1)\cdot\lambda_{Sind} \\ &= A_N^K\cdot\lambda_{Sind}^K\cdot\prod_{i=1}^{K-1}MDTS_{1ooi} \\ &= A_N^K\cdot\lambda_{Sind}\cdot\prod_{i=1}^{K-1}\left(\lambda_{SUind}\cdot\left(\frac{T_1}{i+1}+MRT_S\right)+\lambda_{SDind}\cdot MTTR_S\right) \end{aligned} \quad (4.47)$$

$$STR_{KooN}^{CCF}\approx p_0(\infty)\cdot\left(\beta_{SU}\lambda_{SU}+\beta_{SD}\lambda_{SD}\right)\approx\beta_{SU}\lambda_{SU}+\beta_{SD}\lambda_{SD} \quad (4.48)$$

The general expression of STR_{KooN} can finally be written as:

$$STR_{KooN} = A_N^K \cdot \lambda_{Sind} \cdot \prod_{i=1}^{K-1} \left(\lambda_{SUind} \cdot \left(\frac{T_1}{i+1} + MRT_S \right) + \lambda_{SDind} \cdot MTTR_S \right) + \left(\beta_{SU} \lambda_{SU} + \beta_{SD} \lambda_{SD} \right) \tag{4.49}$$

Note that for *N*oo*N* configurations with $N > 1$, we have to use λ_S instead of λ_{Sind} in Eqs. (4.45) and (4.49), since no CCFs to be considered for the safe failure of the last channel.

By combining Eqs. (4.49) and (4.45), we can find:

$$PFS_{KooN} = STR_{KooN} \cdot MDT_{sd} \tag{4.50}$$

Furthermore, the Mean Time to Failure-spurious ($MTTF_{spurious}$) is a redundant indicator with respect to STR_{KooN} as indicated in (ISA-TR84.00.02-2002, 2002):

$$MTTF_{spurious}^{KooN} = \frac{1}{STR_{KooN}} \tag{4.51}$$

Finally for the entire SIS, we have:

$$PFS_{avg}^{SIS} \approx PFS_S + PFS_{LS} + PFS_{FE} \tag{4.52}$$

$$STR_{SIS} \approx STR_S + STR_{LS} + STR_{FE} \tag{4.53}$$

4.2.3 Results comparison

Now, the previously deduced expressions are used to obtain quantitative values for the PFS_{KooN} and STR_{KooN} of some conventional configurations. The results that are gathered in the following two tables are compared to those obtained from the related multi-phase Markov models. The examination of the theses tables shows that our proposed expressions are very close to those obtained from the Markov models. For instance, Fig. 4.4 depicts the multi-phase Markov model and its corresponding classical one for a 2oo2 architecture, while Fig. 4.5 shows the values issued from their treatment. In Fig. 4.4 the probabilities of the states at the beginning (b_i) of the period (phase) *i* are deduced from the ones obtained at the end (e_{i-1}) of the previous period ($i-1$) as follows: $p_1(b_i)= p_1(e_{i-1}); p_2(b_i)= p_2(e_{i-1})+ p_3(e_{i-1}); p_3(b_i)=0; p_4(b_i)= p_4(e_{i-1})$.

We can easily notice that the average value of PFS_{2oo2} and STR_{2oo2} given by the multi-phase models are very close to the steady states (maximum) values of the classical model.

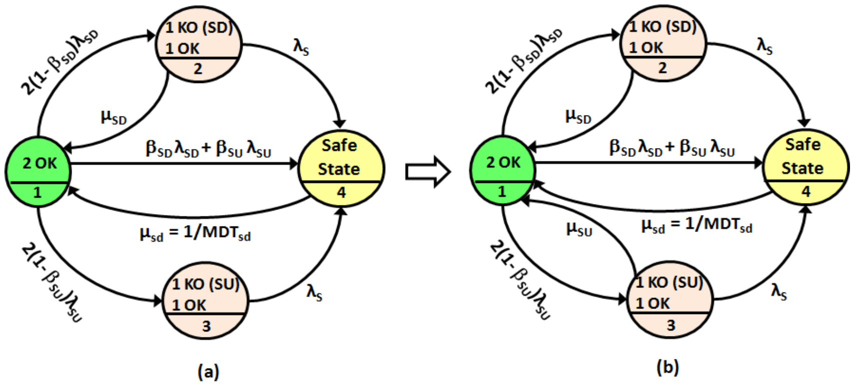


Fig. 4.4 Markov models for 2oo2 configuration: (a) multi-phase and (b) approximated models

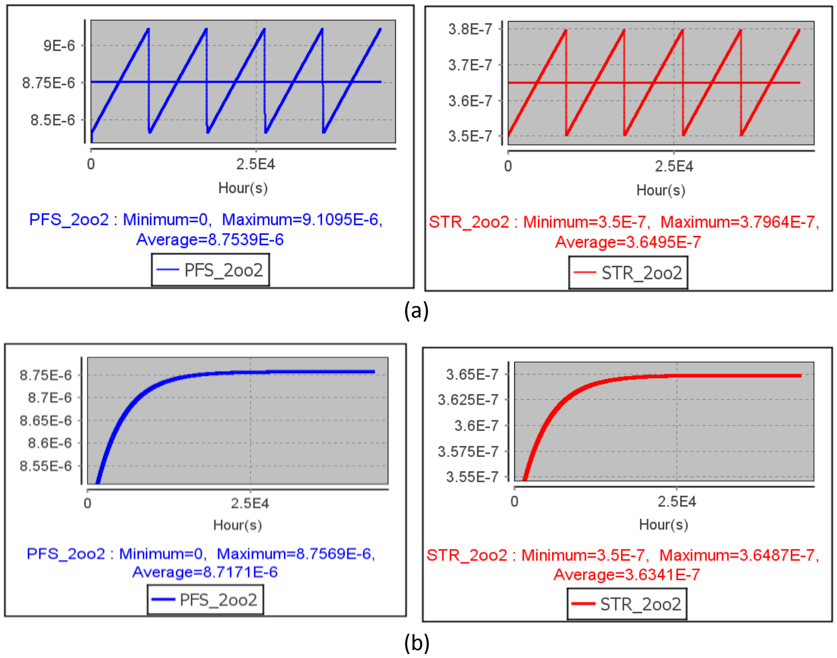


Fig. 4.5 *PFS(t)* and *STR(t)* for 2oo2 architecture obtained from: (a) multi-phase and (b) approximated models

It should be noted that Fault trees do not treat correctly the behavior of *K*oo*N* architectures with $K > 1$ when it comes to safe failures because the last failure (detected or not) being the monitored system in a safe state, in which the repair laws for the *K*oo*N* channels change their initial properties. This problem is similar to the case of dependency in the calculation of repairable systems' reliability. However, Fault trees give good approximate results for (only) STR_{KooN} as reported in Table 4.9. This is explained by the fact that the repair from the safe state slightly affects the STR_{KooN} values, since the safe failures' rates are very low compared to $1/MDT_{sd}$.

Table 4.8 Results related to PFS_{avg} for different *K*oo*N* architectures

λ_S = 2.5E-6/h, DC_S = 0.6, $MTTR_S = MRT_S$ = 8 h, MDT_{sd} = 24 h, T_1= 8760 h and $\beta_{SU} = 2\beta_{SD}$ = 0.2				
	Eq. (4.45)		**Markov models**	
	PFS^{ind}	PFS_{KooN}	PFS^{ind}	PFS_{KooN}
1oo1	6.000E-05	6.000E-05	5.996E-05	5.996E-05
1oo2	1.032E-04	1.116E-04	1.031E-04	1.115E-04
2oo2	4.225E-07	8.822E-06	4.169E-07	8.754E-06
1oo3	1.548E-04	1.632E-04	1.547E-04	1.630E-04
2oo3	1.090E-06	9.490E-06	1.068E-06	9.462E-06
1oo4	2.064E-04	2.148E-04	2.062E-04	2.146E-04
2oo4	2.180E-06	1.058E-05	2.117E-06	1.051E-05

Table 4.9 Results related to *STR* for different *K*oo*N* architectures

λ_S = 2.5E-6/h, DC_S = 0.6, $MTTR_S = MRT_S$ = 8 h, MDT_{sd} = 24 h, T_1= 8760 h and $\beta_{SU} = 2\beta_{SD}$ = 0.2						
	Eq.(4.49)		**Markov models**		**Fault tree**	
	STR^{ind}	STR_{KooN}	STR^{ind}	STR_{KooN}	STR^{ind}	STR_{KooN}
1oo1	2.500E-06	2.500E-06	2.499E-06	2.499E-06	2.499E-06	2.499E-06
1oo2	4.300E-06	4.650E-06	4.299E-06	4.649E-06	4.299E-06	4.649E-06
2oo2	1.760E-08	3.676E-07	1.739E-08	3.649E-07	1.503E-08	3.650E-07
1oo3	6.450E-06	6.800E-06	6.449E-06	6.799E-06	6.449E-06	6.799E-06
2oo3	4.542E-08	3.954E-07	4.453E-08	3.945E-07	4.488E-08	3.948E-07
1oo4	8.600E-06	8.950E-06	8.598E-06	8.948E-06	8.598E-06	8.948E-06
2oo4	9.084E-08	4.408E-07	8.830E-08	4.382E-07	8.934E-08	4.393E-07

4.3 Conclusion

A set of generalized analytical expressions that can be used to evaluate the SIS performance in terms of both safety and operational integrity have been developed in this chapter. The key benefit of such equations is their simplicity and comprehensiveness, since they could be implemented directly for any number of components wired in any *K*oo*N* manner without the need to employ the corresponding reliability tools that are complicated for those who are unfamiliar with their use. The validity of those proposed formulas has been proved through the various conducted comparisons between the results they yield and those of the widely accepted ones and even those of the related reliability tools.

Definitely, all the conducted formulas remain within the context of approximations, the reality that conspicuously returns to the different assumptions and simplifications that have been taken to make possible and facilitate the modeling assignment, which is an ordinary issue for the various kinds of modeling of most of the real world phenomena and systems. However, this subject will be discussed in following chapter. Also, the obtained analytical expressions will be used as a foundation for the subsequent chapter.

5. PARAMETRIC UNCERTAINTY AND SENSITIVITY ANALYSIS

In parallel with Route 1_H, which is discussed in chapter 3, the IEC 61508 provides another way to achieve the architectural constraints' requirements, called Route 2_H. Choosing this route requires the consideration of data uncertainties in the estimation of PFD_{avg} and *PFH*, and ensuring that there is a confidence greater than 90% that the target failure measure is achieved. Indeed, there are many other points that must be respected in this route like the exigency of employing data based on field feedback for elements in use in a similar application and environment, and collected in accordance with the international standards in this area. However, data uncertainty in the IEC 61508 standard is handled within the probabilistic framework.

In the literature, the focus on the subject of treating the different types of uncertainty regarding the estimation of the various performance indicators of SISs is limited to a small number of contributions, while sensitivity analysis is almost absent. For instance, the so-called enhanced Markov analysis (a combination of Markov analysis and uncertainty analysis via the MC analysis and statistical sensitivity analysis) is used in (Rouvroye, 2001) to calculate the *PFD*. In (Sallak, 2007), it is proposed to use the fuzzy Fault trees to evaluate the PFD_{avg}, where triangular fuzzy numbers are used to model the imprecision in failure rates. In the same reference, some probabilistic importance factors are adapted to be used in the fuzzy framework. The problem of imprecision in the values of β and *DC* for the estimation of *PFD* is addressed in (Mechri, 2011) by suggesting several approaches based on the use of Fault trees and Markov models. In the former tool, uncertainty related to β is represented by: a) a triangular fuzzy number, and b) a probability box (P-box), while in the second, uncertainty associated with β and *DC* is treated as: a) intervals, and b) fuzzy numbers represented by α - cuts and then propagated by means of interval analysis. Additionally, the so-called safety-related uncertainty is introduced in (Xu, et al., 2012) and different types of uncertainty in PFD_{avg} estimate are discussed in (Jin, et al., 2012).

The main purpose of this chapter is to describe the current accepted practice in terms of uncertainty and sensitivity analysis and the commonly employed methods and tools in handling such aspects to adopt the ones that fit the specificity of SISs, which is governed by the nature of the involved parameters and data, practicality, usefulness, etc.

5.1 Uncertainty analysis

For several reasons, scientists and engineers employ the scientific modeling, may be to understand a complex phenomenon, to forecast the behavior of a specific system or just to avoid the risky and efforts-consuming real experiments. However, it is well known that the scientific modeling is often a quite complex task that passes through several stages and requires the intervention of several factors and data. This complexity obliges the modeler to make some assumptions, idealizations, and approximations and use inappropriate factors and data. Even though such practices are very helpful at the outset by facilitating the task, unfortunately they accumulate at the end to form the main contributor that affects the credibility of the model. Consequently, the so-called *uncertainty analysis* (UA) has been found to fill these gaps and build strong foundations for any decisions that might be taken on the basis of the results of such modeling.

5.1.1 Definition

In metrology, the term *uncertainty of measurement* is widely used and addressed by several standards. The Guide to the Expression of Uncertainty in Measurement (GUM, 2008) defines this term in its “Annex D” as an expression of the fact that, for a given measurand (quantity to be measured) and a given result of measurement of it, there is not one value but an infinite number of values dispersed about the result that are consistent with all of the observations and data and one’s knowledge of the physical word, and that with varying degrees of credibility can be attributed to the measurand. Another definition was introduced in (VIM, 1993) and also taken in the previously listed guide considers the measurement uncertainty as a non-negative parameter (standard deviation, the half width of an interval having a stated coverage probability,…) characterizing the dispersion of the *quantity values* being attributed to a measurand, based on the information used. Moreover, uncertainty in (ISO 3534-1, 2006) is an estimate attached to a test result which characterizes the range of values within which the true value is asserted to lie.

Let us move to the nuclear industry, where the importance of assessing the impact of uncertainties has been highlighted by several standards and references such as (NRC, 2002; NRC, 2007; ASME/ANS, 2009; NUREG-1855, 2009). For (IAEA, 2008), uncertainty is the measure of scatter in experimental data or calculated values, which is expressed by an interval around the true mean of the parameter resulting from the inability to either measure or calculate the true value of that parameter (scatter). From all of those definitions we can conclude that uncertainty characterizes a collection of the possible interpretations that a specific item may take, which originally should be unique but for many undesired reasons (errors, lack of knowledge…) it has been dispersed.

5.1.2 Classification of uncertainty

The classification of uncertainty defer from one domain to another. Thus, (Thunnissen, 2003; Hayes, 2011), provide a general inspection on how to classify them within different fields.

However, by checking a large number of references such as (NRC, 1998; Stamatelatos, 2002; Durga Rao, et al., 2007; Da-Veiga, 2007; Helton, et al., 2008; Swiler, et al., 2009; National Research Council, 2009; NUREG-1855, 2009; Helton, et al., 2011) it seems that splitting uncertainties into *aleatory* and *epistemic* is the common current practice and the most accepted classification.

At this point, it should be noted that several documents, such as (Mokhtari, et al., 2005; Wu, et al., 2004) consider that uncertainty is related to the lack of knowledge and therefore it includes only the epistemic one, whereas the term *variability* is used instead of aleatory uncertainty. In addition, (Kiureghian, et al., 2009) draws attention to the fact that perhaps all the uncertainties are epistemic, while the aleatory ones are temporal and they will disappear as soon as the modeler learn about all the missing variables and the exact forms of models or even by explaining the basic variables through exact predictive models.

- **Aleatory**

Inherent randomness is extensively used to describe this category. Indeed, from this short description two important facts can be concluded: a) aleatory uncertainties are absolutely related to the nature of the phenomenon or the system itself, so b) there is no way to reduce them and assessing their contribution in the overall uncertainty is the only thing could be done. Furthermore, the reader should be aware that many other names are used to describe this category such as stochastic uncertainty, irreducible uncertainty or just variability as it was mentioned before.

- **Epistemic**

This time, *lack of knowledge* is the used description of this type of uncertainties. Actually, blaming the intrinsic nature of the phenomenon or the system is far from reality here, contrarily the elemental sources of such uncertainties lie in the incapability to obtain the necessary information. Accordingly, when the appropriate and sufficient information become obtainable this type of uncertainties will simply vanish. This category also could be found in the literature under other names such as subjective uncertainty and reducible uncertainty.

Another categorization of uncertainty is currently used in many domains and more especially within the probabilistic risk assessment (PRA) in the nuclear industry. In this latter, uncertainties are decomposed into *model*, *completeness* and *parameter* (NRC, 1998; EPRI, 2006; NUREG-1855, 2009).

- ✓ *Model uncertainty*: Complexity of the system to be studied, mathematical limitations and relationship between the different elements of the model are a sample of what can lead to make approximations, assumptions and/or idealizations that indeed will falsify the real state of the relevant system. Furthermore, the user may find himself forced to choose between two or more alternative models, then logically he has to a) use all of them and try to find a way to compare them, which is quite complicated and often hard to realize, b) subjectively choose one among the different alternatives, what creates the risk of picking out the least adequate, or c) use the so-called *consensus model*, which is sometimes insignificant, first because the interpretation of the term "consensus" and then because in many cases all the alternatives are consensus.

- ✓ *Completeness uncertainty*: Neglecting some important issues (states, factors, modes…), whether purposely or not, has its own involvement in the overall uncertainty. Eliminating the impact of the imperfect repairing on the unavailability of an automated system could be considered as an example of this kind of uncertainties. In fact, the confusion between completeness uncertainties and the model uncertainties, is always present, thus the user can consider all the residual uncertainties that was not included in the model uncertainties as part of this category.
- ✓ *Parameter uncertainty*: This type of uncertainties is completely associated with the availability, nature and quality of data used for the input parameters. Data are becoming more and more available, but actually this is only true for certain general and more famous factors. We can take the case of CCF events models as an illustrative example here, while some of those models are originally designed to use component based data, which are almost unreachable, so the user is obliged to extract them from the available system based data. Additionally, the rarity of the occurrence of some events and the human mistakes are capable to significantly affect the quality of such data. However, the existing ways to represent the parameter uncertainties will be discussed hereafter.

5.1.3 Representation of uncertainty

Starting by the aleatory uncertainties, which it became clear from their description that they have a random nature, so using the probabilistic models is widely regarded as the proper way to deal with them. By the way, within many fields such as process and nuclear industries it is ordinary to employ the probabilistic framework to assess risks that principally treat the random character associated with some relevant events and phenomena.

Regarding the epistemic uncertainties, in addition to the probability theory that faces criticism about its capability to handle this type of uncertainties, different ways have been developed to deal with them, namely: *interval analysis*, *probability bounds analysis*, *fuzzy sets theory*, *possibility theory*, *rough sets theory* and *Dempster-Shafer theory*.

Undoubtedly, model uncertainties have a large involvement, if not the largest in the overall uncertainty, but their complications make them so hard to address or at least to create a common manner or corner from which the analyst within a given field can commence to find the suitable way to manage this type of uncertainties. This fact is reflected by the scarcity of works that deals with such matter. Actually, the case of completeness uncertainties is even worse, because as mentioned in (EPRI, 2006), they entail many unknowns, so it is difficult to describe them and to develop a coherent framework for them. However, this does not negate the fact that many contributions have been proposed to deal with these two types of uncertainties such as: (Zio, et al., 1996; EPRI, 2006; NUREG-1855, 2009; Ferson, 2014) and some others investigated in (Apostolakis, 1989).

Since the parameter uncertainties can be aleatory and/or epistemic, their treatment must depend on that. In what follows we choose some of the commonly used methods and approaches for analyzing uncertainties to be further discussed. Ultimately, it should be noted that some of the proposed ways to deal with the models uncertainties are relatively similar to those used to represent the parametric uncertainties.

- **Probability theory**

Since the probability theory is widely used in various themes, it sounds that there is no need to recall its basics that could be found in numerous sources such as (Kolmogorov, 1956; Feller, 1968; Finetti, 1975). Instead, we enter straightly into the review of one of the most effective methods and applications of this theory that has proved its worth and benefits within many aspects and of course representing uncertainty is one of them. This method was devised in the forties of the twentieth century and known as *Monte Carlo* (MC) *simulation*.

The importance of Monte Carlo simulation lies in its ability to treat the difficult issues that the traditional methods cannot do anything in front of such complexity. Basically, this method aims to build the probability distribution of the output (which characterizes its uncertainty) by propagating a certain number of trails that are sampled from the of input parameters' probability distributions through the relevant model. Generally, the following steps constitute the skeleton of MC simulation:

1) Drawing on the available knowledge, identify the pdf (uniform, lognormal, exponential…) of each input parameter (or the joint distribution for the dependent input parameters). This step could be carried out by means of several techniques, such as: *method of moments* and *maximum likelihood*.
2) Generate a sample of size n from the distribution of each input parameter employing one of the existing sampling techniques. It is well known that the large number of runs is the biggest limitation of MC simulations and finding a reasonable number that comprises between the computation time and the obtained results' quality is usually problematic. However, as it is mentioned in (JCGM, 2008), choosing a values of n that is large (e.g., 10^4 times) compared with $1/(1-p)$ is expected to provide a $100p$% coverage interval for the output.
3) Evaluate the model n different times using the results of the previous step will merely build the output's probability distribution, that of course hold the mean, the standard deviation,…etc, or in a few words, the uncertainty in the output.

Let us go back to the second step where several techniques are devoted to handle such task, for instance we can mention the *importance sampling*, *stratified sampling* and *quasi-random* *sampling*. At this stage, the focus is on two well-known techniques, which are the *random* and *Latin hypercube* ones:

- ✓ *Random sampling*: It is the original sampling technique that is based on generating the random sample from a specific distribution employing random numbers, while each element (individual) has the same chance to be selected. Definitely, computers are deterministic devices, so they are completely incapable to generate random numbers like the roulette wheels for example or the physical methods in general and to defeat this matter scientists have developed a deterministic way to generate the so-called *pseudorandom* numbers (using for example the Linear Congruential Generator) that effectively replace the random ones. Actually, the uniform distribution in the interval [0,1) plays a role of fundamental importance since sampling from this distribution allows obtaining random variables obeying any other distribution (McGrath, 1975), via the different methods of transformation like the *inverse transform*, *composition*, *convolutio*n and *acceptance-rejection* (see (Zio, 2013 (a)) for further reading). According to (EPA QA/G-5S, 2002), the advantages of this design are: a) it provides statistically unbiased estimates of the mean, proportions and variability, b) it is easy to understand and easy to implement and c) sample size calculations and data analysis are very straightforward. The biggest disadvantage of this technique is the difficulty of finding a compromise between the computation time and good coverage of the corresponding space.
- ✓ *Latin hypercube sampling*: First introduced in (McKay, et al., 1979), this sampling technique has the same principle as the so-called stratified sampling (without replacement) whose advantages are twofold: a) covering all the input space and b) less runs are needed than the previously discussed technique. The key idea is: after dividing the range of each x_j into n disjoint strata with equal marginal probability ($1/n$), employ the random sampling to take one value from each stratum of each x_j afterward randomly combining those obtained values to form a sample of n elements, which allows us to simulate the corresponding model n different times.

- **Dempster-Shafer theory**

Actually, this theory was initiated first in (Dempster, 1967) and completed later in (Shafer, 1976) to overcome many drawbacks in the traditional *Bayesian theory* of probability, which have long criticized and judged inadequate in numerous opportunities. As pointed out in (Xu, et al., 2013), Dempster-Shafer theory (DST) is one of the primary tools for knowledge representation and uncertain reasoning.

In this theory, instead of assigning precise probabilities to singleton elements, we can gain more flexibility in terms of considering evidence associated with a set of elements and then dealing with intervals that contain those traditional (precise) probabilities.

By the way, as stated in (Rakowsky, 2007), the beginning of the nineties of the last century witnessed the very first contributions in employing this theory within the fields of reliability and safety, as an example we mention (Guth, 1991), where this theory was used to handle imprecision and vagueness in Fault Tree analysis.

To comprehend the concept of this theory let us consider the set (*frame of discernment*) *Θ* that includes *N* possible hypotheses as represented in Eq. (5.1).

$$\Theta = \{H_1, H_2, ..., H_N\} \qquad (5.1)$$

Thus, $P(\Theta)$ is its power set that is consisted of 2^N propositions:

$$P(\Theta) = \{\phi, \{H_1\}, \{H_2\}, ..., \{H_N\}, \{H_1, H_2\}, \{H_1, H_3\} ... \Theta\} \qquad (5.2)$$

Furthermore, three main functions characterize this theory:

✓ *Basic probability assignment or mass function (bpa or m)*: assigned to each element *A* of the power set $P(\Theta)$ and according to (Klir, et al., 1999) it represents the proportion of all relevant and available evidence that supports the claim that a particular element of *Θ* belongs to the set *A* but to no particular subset of *A*:

$$m : P(\Theta) \to [0,1] \qquad (5.3)$$

where: $m(\phi) = 0$ and $\sum_{A \in P(\Theta)} m(A) = 1$.

The element *A* is called *focal element* if $m(A) > 0$.

From this latter concept, the following two non-additive metrics can be resumed that represent the lower and upper of an interval, which in turn represents the uncertainty relevant to *A* as shows Fig. 5.1.

✓ *Belief (Bel)*: represents the lower limit of the interval and it can be defined as follows:

$$Bel(A) = \sum_{B \subseteq A} m(B) \qquad (5.4)$$

where, *B* is a subset of *A.*

✓ *Plausibility (Pl)*: represents the upper limit of the interval and it can be calculated as follows:

$$Pl(A) = 1 - Bel(\overline{A}) = \sum_{B \cap A \neq \phi} m(B) \qquad (5.5)$$

where $\bar{A}$ is the compliment of *A.*

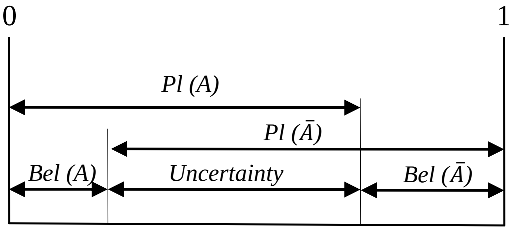


Fig. 5.1 Relationship between Belief, Plausibility and Uncertainty

The original way to fuse information obtained from multiple sources (that are assumed to be independent) within the same frame of discernment is known as *Dempster's rule of combination*. Let m_1 and m_2 to be two basic probability assignments, then their combination (joint) m_{12} could be obtained as follows:

$$m_{12}(A) = \begin{cases} 0 & if \quad A = \phi, \\ \dfrac{\sum\limits_{B \cap C} m_1(B) m_2(C)}{1 - K} & otherwise \end{cases} \tag{5.6}$$

where, $A \neq 0$, $m_{12}(\phi) = 0$ and $K = \sum\limits_{B \cap C = \phi} m_1(B) m_2(C)$ which represents the basic probability related to the conflict.

The elimination the conflict in this rule of combination has exposed it to a lot of criticism, the fact that led to developing several alternatives such as Yager rule (Yager, 1987) and disjunctive consensus rule (Dubois, et al., 1992). The reader is invited to check (Sentz, et al., 2002) (Mousavi, 2012; Martinez, 2012) where deep presentations of those combination rules are provided.

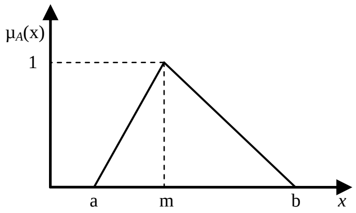
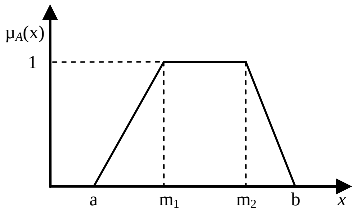
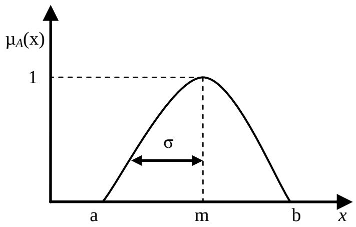
- **Fuzzy sets theory**

This theory was introduced in (Zadeh, 1965), where a fuzzy set is defined as a "class" with a continuum of grades of membership. The membership function that is often denoted by "μ_A" is a key concept in this theory where it is associated with each fuzzy set *A* and it shows the membership grade of each element *x* of the universe of discourse Ω in *A*. Actually, within these types of sets the membership functions are defined in the real interval [0, 1], while in the ordinary sets they are defined in {0, 1}.

A fuzzy number represents any fuzzy set whose membership function is convex (i.e., $\mu_A(\lambda x_1 + (1-\lambda) x_2) \geq \min(\mu_A(x_1), \ \mu_A(x_1))$ for all $x_1, x_1 \in \Omega$ and $\lambda \in [0, 1]$), normalized (i.e., $\exists x \in \Omega, \ \mu_A(x) = 1$) and piecewise continuous.

The following table contains some basic types of fuzzy numbers:

Table 5.1 Triangular, Trapezoidal and Gaussian fuzzy numbers

Type	Mathematical Representation	Graphical Representation
Triangular	$\mu_A(x) = \begin{cases} \dfrac{x-a}{m-a}, & a \le x \le m \\ 1, & x = m \\ \dfrac{b-x}{b-m}, & m \le x \le b \\ 0, & otherwise \end{cases}$	
Trapezoidal	$\mu_A(x) = \begin{cases} \dfrac{x-a}{m_1-a}, & a \le x \le m_1 \\ 1, & m_1 \le x \le m_2 \\ \dfrac{b-x}{b-m_2}, & m_2 \le x \le b \\ 0, & otherwise \end{cases}$	
Gaussian	$\mu_A(x) = e^{\frac{-(x-m)^2}{2\sigma^2}}$	

α - cut or α - level set is another important concept in this theory since it gives the possibility to extend several important properties of the crisp sets to the fuzzy ones through the decomposition of this latter's membership function into a certain number of α - cuts. For a given fuzzy set A and a given real number $\alpha \in [0,\ 1]$, we can obtain the following crisp set, which is the α - cut of A:

$$A^{(\alpha)} = \{A \in \Omega,\ \ \mu_A(x) \ge \alpha\} \tag{5.7}$$

The left and right limits of $A^{(\alpha)}$ are habitually denoted by $A_L^{(\alpha)}$ and $A_R^{(\alpha)}$ respectively.

By means of α –cut sets, we can extract one of the basic ways to carry out fuzzy arithmetic operations via the interval arithmetic:

$$\begin{array}{l} A \to \left[A_L^{(\alpha)}, A_R^{(\alpha)}\right] \\ B \to \left[B_L^{(\alpha)}, B_R^{(\alpha)}\right] \end{array} \left\{ \begin{array}{l} C = A + B \to \left[C_L^{(\alpha)}, C_R^{(\alpha)}\right] \; = \left[A_L^{(\alpha)} + B_L^{(\alpha)}, A_R^{(\alpha)} + B_R^{(\alpha)}\right] \\ C = A - B \to \left[C_L^{(\alpha)}, C_R^{(\alpha)}\right] \; = \left[A_L^{(\alpha)} - B_L^{(\alpha)}, A_R^{(\alpha)} - B_R^{(\alpha)}\right] \\ C = A \cdot B \to \left[A_L^{(\alpha)}, A_R^{(\alpha)}\right] \cdot \left[B_L^{(\alpha)}, B_R^{(\alpha)}\right] \; = \left[C_L^{(\alpha)}, C_R^{(\alpha)}\right] \\ \left\{ \begin{array}{l} C_L^{(\alpha)} = \min\left(A_L^{(\alpha)} \cdot B_L^{(\alpha)}, A_L^{(\alpha)} \cdot B_R^{(\alpha)}, A_R^{(\alpha)} \cdot B_L^{(\alpha)}, A_R^{(\alpha)} \cdot B_L^{(\alpha)}\right) \\ C_R^{(\alpha)} = \max\left(A_L^{(\alpha)} \cdot B_L^{(\alpha)}, A_L^{(\alpha)} \cdot B_R^{(\alpha)}, A_R^{(\alpha)} \cdot B_L^{(\alpha)}, A_R^{(\alpha)} \cdot B_L^{(\alpha)}\right) \end{array} \right. \\ C = A / B \to \left[C_L^{(\alpha)}, C_R^{(\alpha)}\right] = \left[A_L^{(\alpha)}, A_R^{(\alpha)}\right] \cdot \left[1 / B_R^{(\alpha)}, 1 / B_L^{(\alpha)}\right] \end{array} \right. \tag{5.8}$$

- **Probability bounds analysis**

Based on the idea of combining probability theory and interval analysis, this approach, which has been spread through many works like (Ferson, 1994; Ferson, et al., 1996), aims to overcome several limitations and sensitive assumptions in the use of each of them separately. Its main advantage lies in the possibility of dispensing the precise definition of the probability distribution's shape and/or even the dependence relationship between the inputs whenever the available information is not enough to carry out such tasks. Additionally, it has the same capability as the *two-dimensional* (2D) MC simulation in separating aleatory and epistemic uncertainties with less computation time. In probability bounds analysis (PBA), uncertainty is characterized by means of the so-called *probability box* (P-box). A P-box consists of a set of CDFs, that a given variable may take, encased between two characteristic lower ($\underline{F}$) and upper ($\overline{F}$) ones, and as mentioned in (Ferson, et al., 2005) a probability distribution is to a P-box the same way a real scalar number is to an interval. In fact, a P-box can be parametric (i.e., precise distribution with uncertain parameters) or nonparametric (i.e., some insufficient information (e.g., min, max and mean) with an unknown distribution form).

The propagation of uncertainty in the context of PBA could be achieved by means of several methods and algorithms that are developed over the years in many references, like (Yager, 1986; Frank, et al., 1987; Williamson, et al., 1990; Berleant, 1993; Berleant, et al., 1998). Furthermore, (Ferson, et al., 2004; Paredis, et al., 2006) provide an interesting representation and discussion of the various methods of P-boxes' propagation.

The explicit description of the advantages and disadvantages of PBA and many other alternative methods and approaches could be found in (Zio, et al., 2013 (b)).

5.2 Sensitivity analysis

Sensitivity analysis (SA) is a habitual complement of uncertainty analysis. The word "sensitivity" is defined in the Cambridge dictionary as having a strong reaction to something. Simply, sensitivity analysis is intended to measure the strength of that reaction. Actually, one of the extensively accepted definitions of sensitivity analysis that is provided in (Saltelli, et al., 2004) considers this latter as the study of how the variation in the output of a model can be apportioned qualitatively or quantitatively, among model inputs. In fact, the term "input" in this definition should not be seen only as the values of the input parameters that feed the model, but it may contain other meanings like an importance parameter associated with certain assumption, approximation or hypothesis. Several references have discussed the why of conducting such analysis like (Pannell, 1997), where a list of nineteen reasons has been provided that have been clustered into four broad groups, namely: decision making or development of recommendations for decision makers, communication, increased understanding or quantification of the system, and model development. Also, the goal of SA according to (Hamby, 1994) is to determine:

- ✓ which parameters require additional research for strengthening the knowledge base, thereby reducing output uncertainty;
- ✓ which parameters are insignificant and can be eliminated from the final model;
- ✓ which inputs contribute most to output variability;
- ✓ which parameters are most highly correlated with the output;
- ✓ once the model is in production use, what consequence results from changing a given input parameter.

In the context of sensitivity analysis, a large number of methods have been developed to keep pace with the degree of the relevant model sophistication and/or the desired objectives of the study. At this level, we will be focusing on the traditional and probabilistic ones. As a matter of fact, various criteria can be relied upon to categorize those methods. For instance, in (Frey, et al., 2002) SA methods could be: mathematical, statistical or graphical; in (Hamby, 1994) they are addressed in three groups: methods operate on one variable at time, methods rely on the generation of an input matrix and an associated output vector and methods require a partitioning of a particular input vector based on the resulting output vector; also, SA methods could be considered as either qualitative (screening) or quantitative; another widely used classification, which will be adopted throughout this work, splits them into local and global (Homma, et al., 1996; Cacuci, 2003; Saltelli, et al., 2008). Another category called *screening experiments* (e.g., Morris method (Morris, 1991)) is added to these latter two ones in some references like (JRC-ISIS-SAIE-UASA, 1999).

5.2.1 Local sensitivity analysis

Drawing on the *one-at-a-time* (OAT) concept, the main principle of this category is estimating the effect of the variation of the input values around a specific nominal (baseline) point in the input domain. Several references have explicitly investigated the local SA methods, for example we can draw attention to (Frey, et al., 2002; Cacuci, 2003; Mokhtari, et al., 2005). However, the easiest way to conduct the local SA is computing the first order partial derivative of the output with respect to specified factor at a specified value.

The limitations of the one-at-a-time approach and local SA methods have been excessively investigated in the literature that could be concluded in their inability to efficiently handle the nonlinearity and highly uncertain inputs, whereas the simplicity is the biggest advantage of such methods.

5.2.2 Global sensitivity analysis

Unlike the local methods, the ones within this category are capable to estimate the effect of the variation of an input (s) while all the other inputs are varying (or even OAT) within their entire domain simultaneously. A description of some of the widely used global sensitivity methods is provided in the Appendix.

It should be noted that for further information, description and comparison between the various SA methods, the reader is advised to check (Hamby, 1994; Frey, et al., 2002; Confalonieri, et al., 2010; Mazzilli, 2011).

Finally, it is important to note that some of the new (uncertainty) methods like PBA and DST are regarded able to perform global sensitivity analysis with more comprehensiveness than those traditional ones and less complexity and efforts are involved. This subject is addressed in (Ferson, et al., 2006 (a); Ferson, et al., 2006 (b); Aughenbaugh, et al., 2007). However, most of these methods are OAT, the matter that should be taken into account.

5.3 Treatment of parametric uncertainty and sensitivity analysis in the context of safety instrumented systems

As we have seen the previous chapters, several parameters with different natures are involved in estimation of the different SIS performance indicators. This diversity in the input parameters' nature in addition to the availability and quality of the associated data, the factors that vary from an application to another, requires the careful selection of the appropriate way to incorporate uncertainty, where several (contradict) aspects are involved and should be compromised, such as: suppleness in the depiction of the information, applicability, simplicity, consideration of dependency, and the amount and importance of the obtained results.

In what follows, the possible situations that may be encountered in the process of assessing the performance of SIS in terms of the used data to feed the related models are scrutinized, and based on that we suggest to employ the method that is regarded as the apt one to handle parametric uncertainty and therefore (but not necessarily) the one of sensitivity analysis.

5.3.1 Case 1: All the probability distributions of all the input parameters can be defined

In the case where the analyst has enough information to construct (precise) probability distributions for all the input parameters and designate the dependence relationships (if they exist) between them, then employing MC simulation is regarded as one of the most suitable ways to handle both uncertainty and sensitivity. Actually, the problem of computation time cannot be considered imperative with the existence of the various advanced sampling techniques, especially in the context of SIS where the number of the involved uncertain parameters is generally small (< 10).

At this stage, let us consider a subsystem of a SIS composed of three identical components (ESD valves) wired in a 2oo3 configuration. Knowing that the subsystem is subject to DU failures, CCF events, PST, and PT, we can assess its performance in terms of safety integrity through the usage of the proposed Eq. (4.31) for PFD_{avg} and Eq. (4.33) for PFH. The required data is considered available to obtain the related distributions that are depicted in Table 5.2.

Table 5.2 Data associated with the 2oo3 subsystem (probability distributions)

Parameter	Value
$\boldsymbol{m}$	6
$\boldsymbol{DC}$	*Triangular* (0.4, 0.5, 0.6)
$\boldsymbol{T_{ST}}$ (h)	*Uniform* (1400, 1500)
$\boldsymbol{\lambda_D}$ (h^{-1})	*Lognormal* (μ=-13.2, σ=0.87)
$\boldsymbol{\theta}$	*Uniform* (0.4, 0.7)
$\boldsymbol{\beta_{ST}}$	*Triangular* (0.01, 0.055, 0.1)
$\boldsymbol{\beta_{PT}}$	*Triangular* (0.1, 0.15, 0.2)

In the case where uncertainties are not taken into account, the mean values of those distributions would be employed to get the following results:

Table 5.3 PFD_{avg} and PFH of the 2oo3 subsystem (without uncertainty)

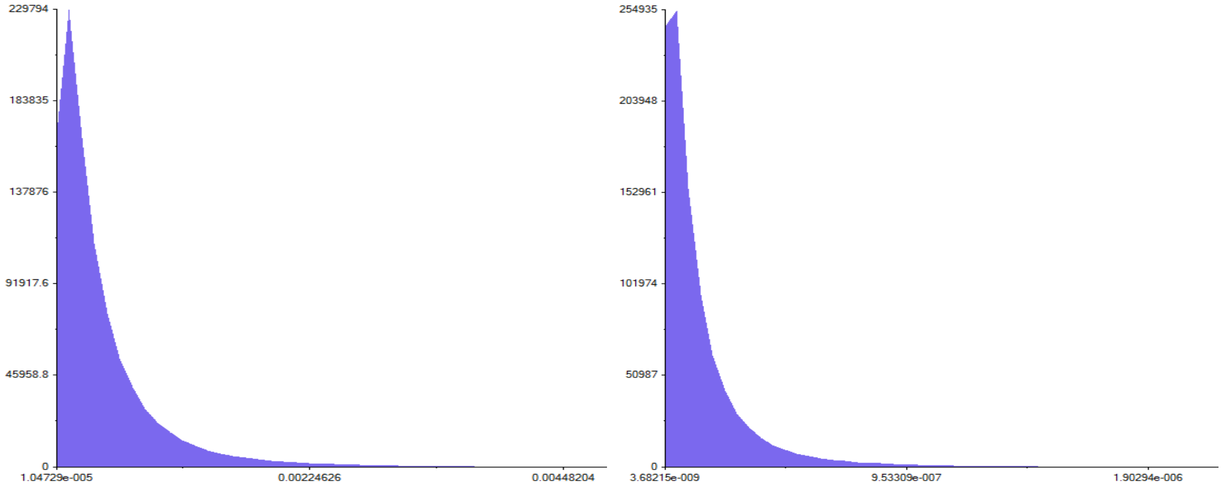
	Eqs. (4.31) and (4.33)	Fault tree
$\boldsymbol{PFD_{avg}}$	4.5445E-4	4.5321E-4
$\boldsymbol{PFH}$ (h^{-1})	1.5210E-7	1.5182E-7

Besides the closeness between the results of the analytical formulas and the ones of Fault tree, the fact that validates the use of such equations once again, we can notice that the subsystem can guarantee a SIL 3 in the case of low demand mode and SIL 2 in the high demand mode.

In purpose of propagating the related uncertainties, we apply MC simulation with some of its various techniques that are discussed previously, the task that can be achieved via the Simlab software (Simlab 2.2.1), to obtain the following results:

Table 5.4 PFD_{avg} and *PFH* of the 2oo3 subsystem (with uncertainty handled by MC simulation)

	PFD_{avg}			*PFH*		
	mean	variance	[min, max]	mean	variance	[min, max]
Random	4.78E-4	3.64E-7	[1.0473E-5, 1.1190E-2]	1.70E-7	5.59E-14	[3.6821E-9, 4.7518E-6]
Latin Hypercube	4.78E-4	3.47E-7	[7.6766E-6, 1.2395E-2]	1.70E-7	5.61E-14	[3.1218E-9, 5.0355E-6]
eFast	4.77E-4	3.39E-7	[1.0779E-5, 1.2695E-2]	1.69E-7	5.45E-14	[3.3690E-9, 5.0732E-6]
Sobol	4.80E-4	3.60E-7	[1.6635E-5, 9.4857E-3]	1.70E-7	5.82E-14	[5.0557E-9, 3.6819E-6]



(a) (b)

Fig. 5.2 Frequency distribution of: (a) PFD_{avg} and (b) *PFH*

The mean values of PFD_{avg} and *PFH* give the same SILs as in the case of not considering uncertainties, but if we consider that we are in the system level, the selection of route 2_H requires the corroboration that there is a confidence greater than 90% that the target failure measure is achieved. To take into account such requirement, one can evaluate the corresponding CDF at the upper limit of that SIL. In this case, the probability that PFD_{avg} is less than or equal to 1E-3 (the upper limit of SIL 3)[4] is 0.917, while the probability that *PFH* is less than or equal to 1E-6 (the upper limit of SIL 2) is 0.987. By comparing those probabilities with the 0.9 of the standard, one can be confident that the 2oo3 subsystem can ensure a SIL 3 in the low demand mode and SIL 2 in the high demand mode.

In addition to uncertainty analysis, the same operations of MC simulation can yield the following results that represent the sensitivity analysis. The first six measures are obtained via the Latin Hypercube technique with a number of 1E6 runs.

[4] To be more accurate, one must evaluate the CDF at a value that is slightly below the upper limit of the corresponding SIL, let us say 9.9E-4 instead of 1E-3 in this case.

Table 5.5 Sensitivity analysis related to PFD_{avg} of the 2oo3 subsystem (probabilistic framework)

	λ_D	β_{ST}	β_{PT}	DC	θ	T_{ST}
PEAR	9.500E-1 **1**	2.070E-3 **4**	7.990E-2 **2**	-5.640E-2 **5**	-1.470E-1 **6**	2.740E-2 **3**
SPEA	9.649E-1 **1**	1.430E-2 **4**	1.220E-1 **2**	-6.628E-2 **5**	-1.798E-1 **6**	3.360E-2 **3**
PCC	9.670E-1 **1**	6.330E-2 **4**	3.145E-1 **2**	-2.901E-1 **5**	-5.012E-1 **6**	7.200E-2 **3**
PRCC	9.948E-1 **1**	2.410E-1 **3**	7.790E-1 **2**	-6.671E-1 **5**	-8.816E-1 **6**	2.146E-1 **4**
SRC	9.519E-1 **1**	1.590E-2 **4**	8.310E-2 **2**	-7.604E-2 **5**	-1.453E-1 **6**	1.810E-2 **3**
SRRC	9.689E-1 **1**	2.460E-2 **3**	1.232E-1 **2**	-8.881E-2 **5**	-1.852E-1 **6**	2.180E-2 **4**
Fast (first order)	5.722E-1 **1**	1.140E-2 **4**	2.600E-2 **2**	5.500E-3 **5**	2.410E-2 **3**	5.350E-4 **6**
Fast (total order)	9.464E-1 **1**	2.046E-1 **3**	2.183E-1 **2**	1.345E-1 **6**	1.745E-1 **4**	1.352E-1 **5**
Sobol (first order)	8.566E-1 **1**	0 **6**	2.060E-2 **2**	7.176E-3 **4**	7.497E-3 **3**	5.530E-4 **5**
Sobol (total order)	9.480E-1 **1**	9.990E-16 **6**	5.741E-2 **2**	5.049E-2 **3**	1.735E-2 **4**	6.367E-3 **5**

Table 5.6 Sensitivity analysis related to PFH of the 2oo3 subsystem (probabilistic framework)

	λ_D	β_{ST}	β_{PT}	DC	θ	T_{ST}
PEAR	9.554E-1 **1**	3.570E-2 **3**	4.030E-2 **2**	-5.540E-2 **5**	-6.830E-2 **6**	1.160E-2 **4**
SPEA	9.806E-1 **1**	8.280E-2 **2**	7.980E-2 **3**	-6.753E-2 **5**	-8.359E-2 **6**	1.360E-2 **4**
PCC	9.628E-1 **1**	1.967E-1 **2**	1.620E-1 **3**	-2.680E-1 **6**	-2.430E-1 **5**	1.070E-2 **4**
PRCC	9.967E-1 **1**	7.572E-1 **2**	7.108E-1 **3**	-7.444E-1 **5**	-7.457E-1 **6**	2.810E-2 **4**
SRC	9.580E-1 **1**	5.390E-2 **2**	4.410E-2 **3**	-7.480E-2 **6**	-6.736E-2 **6**	2.900E-3 **4**
SRRC	9.847E-1 **1**	9.360E-2 **2**	8.160E-2 **3**	-9.006E-2 **5**	-9.038E-2 **6**	2.300E-3 **4**
Fast (first order)	7.080E-1 **1**	2.340E-2 **2**	2.000E-2 **3**	5.300E-3 **5**	1.260E-2 **4**	2.870E-3 **6**
Fast (total order)	9.629E-1 **1**	2.938E-1 **2**	2.413E-1 **3**	1.794E-1 **5**	2.141E-1 **4**	1.722E-1 **6**
Sobol (first order)	9.003E-1 **1**	0 **6**	4.059E-3 **3**	6.998E-3 **2**	2.368E-3 **4**	4.690E-5 **5**
Sobol (total order)	9.737E-1 **1**	3.890E-16 **6**	1.905E-2 **3**	6.282E-2 **2**	5.382E-3 **4**	2.746E-3 **5**

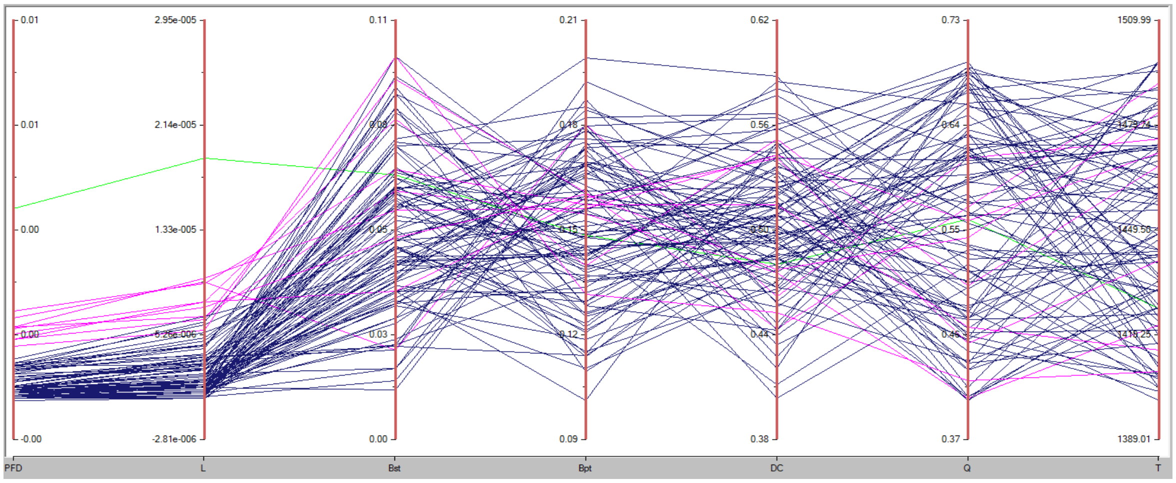


Fig. 5.3 Cobweb plot of PFD_{avg} and its input parameters

The various measures in Table 5.5 and even the cobweb plot of Fig. 5.3 totally agree that PFD_{avg} is primarily sensitive to λ_D, which is the same remark for PFH. However, the inconsistency between those measures for the rest of the inputs (appears as a conflict in their ranks) mainly refers to their related amount of uncertainty which could be considered close to each other.

5.3.2 Case 2: Only bounds

The use of min-max represents one of the easiest and commonly employed ways to represent the uncertain information. Sometimes, it may happen that the only available information about every input parameter is characterized by a simple interval. In such cases, instead of assuming that those parameters are following the uniform distribution and using MC simulation, the matter that could be misleading (see (Ferson, et al., 1996; Baudrit, 2005)), it can be easier and more appropriate to propagate those intervals by means of interval analysis to obtain an interval as an output. Indeed, having an interval as an output may not be very informative or representative (especially in the case of SIS) but the simple operations, clear interpretation and rigorous results are most often guaranteed.

However, it seems interesting to investigate the applicability of DST in such cases by using the so-called *evidential networks* (EN). Actually, the use of such networks in reliability analysis has been addressed in several references like (Simon, et al., 2009 (a); Simon, et al., 2009 (b); Yang, et al., 2012), in this section we will adapt such approach to obtain PFD_{avg} and *PFH*.

Following (Guth, 1991), where the PROBIST (probability binary state) hypothesis is used in the context of DST, it became habitual to consider that $P(\Theta) = \{\{Up\}, \{Down\}, \{Up, Down\}\}$, where $\{Up\}$ represents the normal operation of the item (component or system), $\{Down\}$ represents its failure, while $\{Up, Down\}$ means that the item is (exclusively) in one of the two states without knowing (specifically) which one. The EN of our 2oo3 subsystems is depicted in Fig. 5.4.

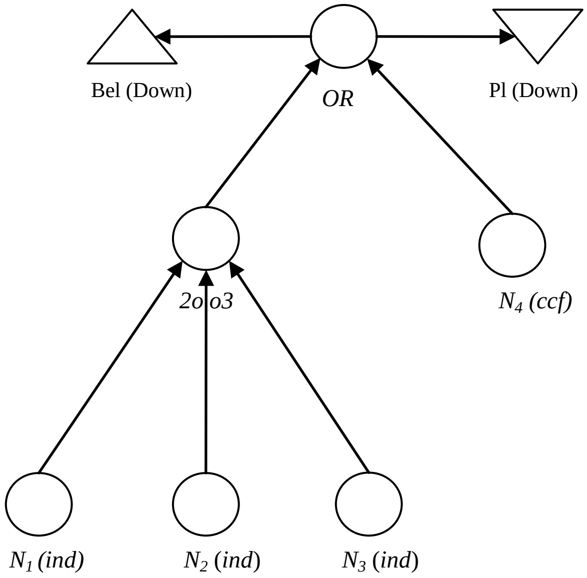


Fig. 5.4 Evidential network of the 2oo3 subsystem

The following table contains the 2oo3 subsystem's data, which is given as intervals.

Table 5.7 Data associated with the 2oo3 subsystem (intervals)

Parameter	Value
$\boldsymbol{m}$	6
$\boldsymbol{DC}$	[0.4, 0.6]
$\boldsymbol{T_{ST}}$ (h)	[1400, 1500]
$\boldsymbol{\lambda_D}$ (h^{-1})	[4.43E-7, 7.73E-6]
$\boldsymbol{\theta}$	[0.4, 0.7]
$\boldsymbol{\beta_{ST}}$	[0.01, 0.1]
$\boldsymbol{\beta_{PT}}$	[0.1, 0.2]

In order to get the a priori belief mass distributions of the root nodes *N1*, *N2* and *N3* we can use Eq. (4.29) for the case of PFD_{avg} and the independent part of Eq. (4.33) for *PFH*, by defining N=K=1. The a priori mass distribution of *N4* could be obtained by means of Eq. (4.30) for PFD_{avg} and the CCF part of Eq. (4.33) for *PFH*. Actually, after defining N=K=1 those equations will not contain any fractions, so there will not be any problem with the denominators and to obtain the results of Table 5.8 it is enough to respect the following constraints, which can be attained by testing if PFD_{avg} and *PFH* are (monotonically) increasing or decreasing with respect to each input parameter.

$$\underline{PFD}_{avg},\ \underline{PFH} = f\ \left(N,\ K,\ m,\ \overline{DC},\ \underline{T}_{ST},\ \underline{\lambda}_D,\ \overline{\theta},\ \underline{\beta}_{ST},\ \underline{\beta}_{ST}\right) \tag{5.9}$$

$$\overline{PFD}_{avg},\ \overline{PFH} = f\ \left(N,\ K\ ,m,\ \underline{DC},\ \overline{T}_{ST},\ \overline{\lambda}_D,\ \underline{\theta},\ \overline{\beta}_{ST},\ \overline{\beta}_{ST}\right) \tag{5.10}$$

Table 5.8 A priori belief mass distributions of the root nodes of the 2oo3 subsystem

		***m*(\{*Up*\})**	***m*(\{*Down*\})**	***m*(\{*UP, Down*\})**
Low demand mode	***N1, N2, N3***	9.887297E-1	2.869045E-4	1.098344E-2
	N4	9.973563E-1	2.319548E-5	2.620465E-3
High demand mode	***N1, N2, N3***	9.999961E-1	1.706436E-7	3.725256E-6
	N4	9.999993E-1	6.556400E-9	7.355436E-7

At this level, we can use BayesiaLab software (Jouffe, et al., 2010), which includes an exact inference method based on junction trees and another approximate one uses the likelihood weighting, in purpose of obtaining the conditional belief mass distributions of the child (non-root) nodes. The conditional belief mass tables of the different gates involved in our 2oo3 subsystem can be found in (Simon, et al., 2009 (b)) (with some rectifications and modifications).

The obtained results are shown in Table 5.9 and Fig. 5.5.

Table 5.9 *PFD_{avg}* and *PFH* of the 2oo3 subsystem (with uncertainty handled by ENs)

	m	***Bel=(_)***	***Pl=(¯)***
PFD_{avg}	2.3442E-5	2.3442E-5	3.0209E-3
PFH	7.0000E-9	7.0000E-9	7.4200E-7

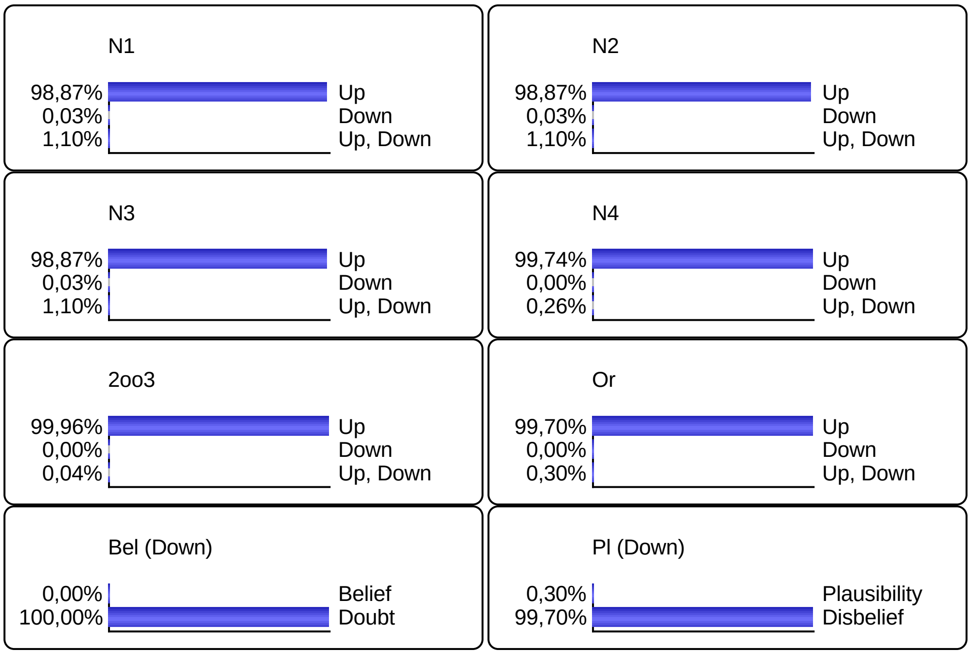


Fig. 5.5 *PFD_{avg}* of the 2oo3 subsystem and its related parameters in the context of evidential networks

Those results indicate that *PFD_{avg}*=[2.34E-5, 3.02E-3] and *PFH*=[7.00E-9, 7.42E-7], which means that, in the worst case, the 2oo3 subsystem can provide SIL 2 for both demand modes.

In fact, we can easily obtain similar results to those of ENs by directly using Eqs. (4.31) and (4.33), once to calculate the lower limit (belief) of the interval and a second one to get its upper limit (plausibility), and definitely, respecting Eqs. (5.9) and (5.10). As an illustration, we have implemented this way to obtain *PFD_{avg}* and this result is [2.35E-5, 3.13E-3], which is very close to the interval obtained via EN. Indeed, the same method can be used to estimate *PFH* and even the performance indicators of the operational integrity (i.e., *PFS_{avg}* and *STR*), the ones that need further efforts if they will be addressed differently.

Concerning, the sensitivity analysis, we can use the subsequent formula, which is provided in (Ferson, et al., 2006 (a)).

$$100\left(1-\frac{unc(T)}{unc(B)}\right)\% \tag{5.11}$$

where, *unc*() in this case is the intervals' width, *B* is the base value of PFD_{avg} or *PFH*, and *T* represents their values with a pinched input to a point value.

By applying this method we can get the following results:

Table 5.10 Sensitivity analysis of the 2oo3 subsystem (inputs as intervals)

	λ_D	β_{ST}	β_{PT}	*DC*	θ	T_{ST}
PFD_{avg}	95.8289 **1**	03.7319 **6**	36.5488 **4**	37.0694 **3**	46.5345 **2**	07.6926 **5**
PFH	96.3409 **1**	15.2826 **5**	22.8401 **4**	39.4241 **2**	22.8565 **3**	01.7586 **6**

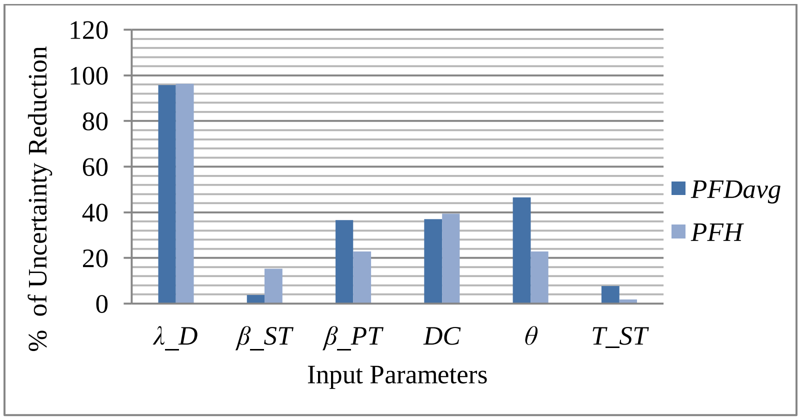


Fig. 5.6 Sensitivity analysis for PFD_{avg} and *PFH* of the 2oo3 subsystem when the inputs are given as intervals

The results show the dominance of λ_D, where pinching it to a point value yields a 95.8% uncertainty reduction in the value of PFD_{avg} and 96.3% in the one of *PFH*.

5.3.3 Case 3: Multi-type parameters

Practically, there is an irrefutable dissimilarity between the various involved input parameters in terms of availability and quality of the associated data. This fact is referred to the inputs' nature and the sources and ways of obtaining their related data. In this context, Table 5.11, which is proposed in (Baudrit, 2005), could be helpful in choosing the appropriate framework to represent the uncertain input parameters depending on the available information without the need to make any baseless assumptions. Consequently, the analyst finds himself in front of a mixture of types of data, whereas some input parameters are considered random variables with or without precisely known probability distributions and parameters, others are simple intervals, and many other ones are characterized by fuzzy numbers. Logically, instead of attempting to adapt them to one format, the matter that can be misleading or cause the loose of some very important characteristics and information, it is much better to deal with them as they are what necessitates the intervention of a combination approach.

Table 5.11 Non-exhaustive list of mathematical representations consistent with the nature of the information (Baudrit, 2005)

When we know	Classical probabilistic representation	Proposed representation
[min, max]	Uniform distribution	Interval
[min, mode, max]	Triangular distribution	Possibility
[min, mean, max]	Beta distribution	P-box
[min, median, max]	Truncated gamma distribution	Belief function
[min, mean, standard deviation, max]	Beta distribution	Possibility
[min, fractiles, max]	Truncated gamma distribution	Belief function
Consequent sample	Empirical distribution function	Empirical distribution function
Poor sample	Test of adequacy to families	P-box
Knowledge of the distribution's shape	Corresponding distribution with estimation of its parameters	P-box
Knowledge of the distribution's shape and intervals on the parameters	2D Monte Carlo	P-box

We propose here to make use of the PBA, which was discussed formerly, with some involvement of MC simulation. Table 5.12 consists of different types of data related to the 2oo3 subsystem.

Table 5.12 Data associated with the 2oo3 subsystem (multi-type data)

Parameter	Value
$\boldsymbol{m}$	6
$\boldsymbol{DC}$	*Triangular (Fuzzy)* [0.4, 0.5, 0.6]
$\boldsymbol{T_{ST}}$ (h)	[1400, 1500]
$\boldsymbol{\lambda_D}$ (h^{-1})	*Lognormal* (μ=-13.2, σ=0.87)
$\boldsymbol{\theta}$	[0.4, 0.7]
$\boldsymbol{\beta_{ST}}$	*Triangular (Fuzzy)* [0.01, 0.055, 0.1]
$\boldsymbol{\beta_{PT}}$	*Triangular (Fuzzy)* [0.1, 0.15, 0.2]

Since some of the inputs are fuzzy numbers and other ones are random variables, the outcome will be a hybrid number (see (Kaufmann, 1986; Cooper, et al., 1995)), which is a nested structure that consists of set of P-boxes. This matter requires the implementation of two probability bounds analyses, one for the bases (support) of the fuzzy numbers and another one for the modal values. The software Risk calc (Ferson, 2002) can be used to propagate such quantities through the corresponding models, but it is important to take into consideration the problem of the repeated parameters to avoid the wide (overestimated) results. However, in an analogous way to the previous case, we can obtain the lower and upper bounds of the P-boxes separately using R (R Software, 2014).

The obtained results are shown subsequently:

Table 5.13 *PFD_{avg}* and *PFH* of the 2oo3 subsystem (with uncertainty handled by PBA)

	PFD_{avg}	***PFH*** (h^{-1})
Mean	[1.652E-4, 5.057E-4, 1.050E-3]	[6.322E-8, 1.744E-7, 3.277E-7]
Min, Max	[1.294E-6, 4.561E-1]	[3.665E-10, 2.274E-4]
90th percentile	[3.440E-4, 1.068E-3, 2.188E-3]	[1.311E-7, 3.634E-7, 6.816E-7]

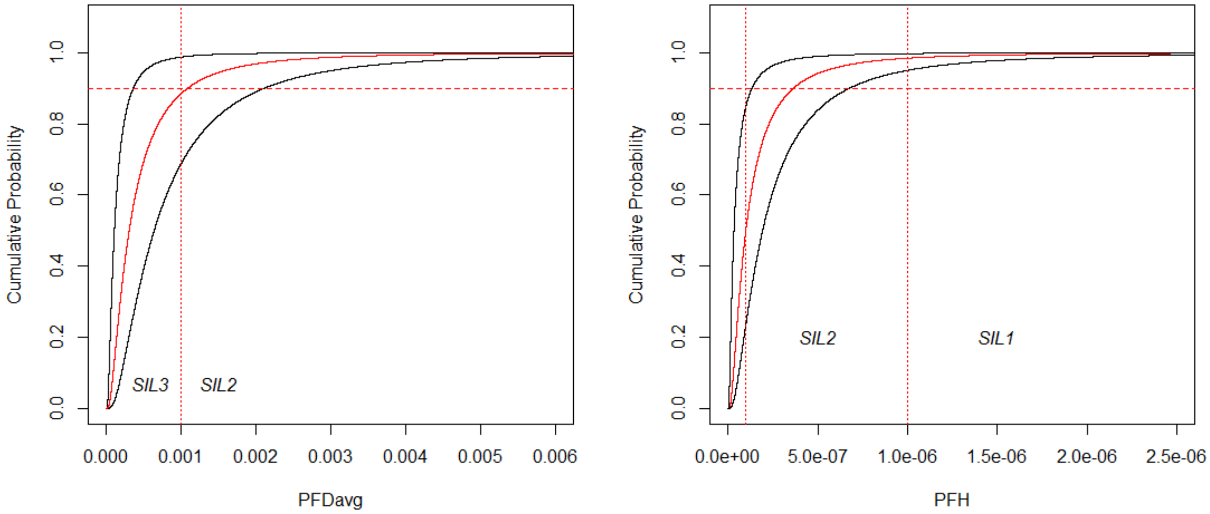


Fig. 5.7 *PFD_{avg}* and *PFH* of the 2oo3 subsystem represented as hybrid numbers (P-boxes)

In Fig. 5.7 the widest (black) P-boxes, which surround all the possible distributions of PFD_{avg} and *PFH*, are obtained through the use of the bases' limits of the fuzzy numbers *DC*, β_{ST} and β_{PT} and the ones of the intervals of the two parameters T_{ST} and θ, while the narrowest (red) ones (can be regarded as the modal P-boxes) are gotten by considering the fuzzy numbers' peaks. The other parameter that has a precise pdf (i.e., λ_D) is included in both cases by sampling its distribution using MC simulation.

As it is shown in Table 5.13, the mean values of PFD_{avg} and *PFH* are triangular fuzzy numbers that cover several SIL zones. By defuzzifying those numbers using the *centroid* method we can get a value of 5.731E-04 for PFD_{avg} and 1.884E-07 (h^{-1}) for *PFH*, which means that the 2oo3 subsystem can provide safety functions with SIL 3 in the low demand mode and SIL 2 in the high demand mode. Apparently, the same results can be obtained by dealing directly with the modal values of those fuzzy numbers.

Over again, if we are in the system level, one needs to take into account the IEC 61508 requirement when route 2_H is selected. At this juncture, we can simply compare the results of the mean values with the ones of the 90th percentiles, which are triangular fuzzy numbers too. Without the need to defuzzify the 90th percentile of *PFH*, we can notice that it favors the mean in assigning a SIL 2 for the corresponding demand mode all over its range. On the other hand, the use of the *centroid* method shows that the 90th percentile of PFD_{avg} is equal to 1.2E-3, which corresponds to a SIL 2. More precisely, the probability that PFD_{avg} is less than or equal to 1E-3 is [0.6749, 0.8882, 0.9893] that could be defuzzified to get 0.8508, which is less than 0.9 of the standard. This means that further improvements must be made to be able to judge that the system is providing SIL 3 in the low demand mode.

Graphically, it can be noted in Fig. 5.7, where the SIL zones are separated by the dotted red (vertical) lines that, for the case of *PFH*, the red dashed (horizontal) line, which designates the 90th percentile, is intersecting all the P-boxes in the SIL2 zone, whereas in the case of PFD_{avg} it is crossing only the left bound of the widest P-box in SIL 3 zone and the other ones (including the modal one) in the zone of SIL 2.

Once more, sensitivity analysis can be performed in a similar way to the employed one in section 5.3.2. This time, *unc*() of Eq. (5.11) is considered as the area of the P-box. Table 5.14 and Fig. 5.8 contain the obtained results:

Table 5.14 Sensitivity analysis of the 2oo3 subsystem (multi-type parameters)

	λ_D	β_{ST}	β_{PT}	*DC*	θ	T_{ST}
PFD_{avg}	85.2759 **1**	04.8763 **6**	46.9907 **3**	43.3436 **4**	54.8349 **2**	08.8015 **5**
PFH	86.0247 **1**	20.8943 **5**	32.4177 **3**	47.1217 **2**	27.0402 **4**	01.7264 **6**

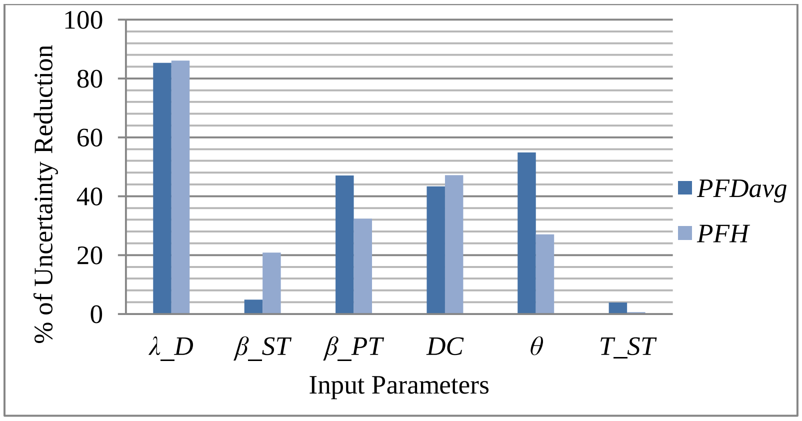


Fig. 5.8 Sensitivity analysis for PFD_{avg} and *PFH* of the 2oo3 subsystem when the inputs are with different natures

Obviously, pinching λ_D to a point value is lessening the uncertainty in the value of PFD_{avg} with an amount that exceeds 85% which could be perceived that the largest share in the resulting uncertainty is aleatory, the thing that can be graphically confirmed, since in Fig. 5.7 the left and right bounds of the P-boxes are almost intersecting each other in their edges (endpoints). Thus, in this case, more efforts on the empirical studies could not be very beneficial in reducing the obtained uncertainty. Actually, the same observations can be said about the case *PFH*.

5.4 Combining Monte Carlo and fuzzy sets approaches

At this stage, another way to handle the parametric uncertainty in the cases where the related data is defined within different frameworks by combining MC simulation and fuzzy sets theory is proposed. Before presenting the suggested approach let us take a SIS whose subsystem S is made up of three pressure transmitters with 1oo3 architecture, the subsystem LS consists of two programmable logic controllers with a 1oo2 configuration, while the subsystem FE is composed of five shutdown valves connected in a 2oo5 way. To assess the performance of this system in terms of safety integrity we can use Eq. (30) for PFD_{avg} and Eq. (31) for PFH that are provided in (Innal, et al., 2015).

Firstly, we apply the MC simulation with 1E+4 runs to propagate the related uncertainty using the data of Table 5.15. The obtained results are summarized in Table 5.16, while the histograms and CDFs of PFD_{avg} and PFH are respectively presented in Figs. 5.9 and 5.10.

Table 5.15 Reliability characteristics of the SIS Elements

Parameters	**Subsystem S:** **1oo3**	**Subsystem LS:** **1oo2**	**Subsystem FE:** **2oo5**
λ_D (h^{-1})	Logn. (–12.5, 0.557)	Trian. (5E–7, 1E–5, 3.67E–6)	Trian. (3E–6,1E–5, 5.33E–6)
DC	Unif. (0.6, 0.8)	Unif. (0.95, 0.99)	Trian. (0.2,0.5, 0.3)
β	Beta (2.33, 4.66) with $0.15 \leq x \leq 0.30$	Unif. (0.01, 0.1)	Unif. (0.1, 0.2)
β_D	Gam. (3.70, 0.027)	Unif. (0.005, 0.05)	Unif. (0.1, 0.2)
MTTR & MRT(h)	Logn. (2.43, 0.21)	Logn. (2.047, 0.4)	Logn. (2.85, 0.34)
T_1 (h)	Constant (4380)	Constant (8760)	Constant (2190)

Table 5.16 Obtained results from the MC approach

Elements	PFD_{avg}	PFH (h^{-1})
S	5.774E–4	5.642E–7
LS	3.577E–5	1.396E–7
FE	6.853E–4	9.157E–7
SIS	Min = 4.118 E–4	Min = 6.144E–7
	Max = 5.753 E–3	Max = 5.724E–6
	Mean = 1.299E–3	Mean = 1.619E–6
	σ = 4.431E–4	σ = 4.691E–7
	$PFD_{05\%}$ = 7.395E–4	$PFH_{05\%}$ = 1.004E–6
	$PFD_{95\%}$ = 2.095E–3	$PFH_{95\%}$ = 2.456E–6

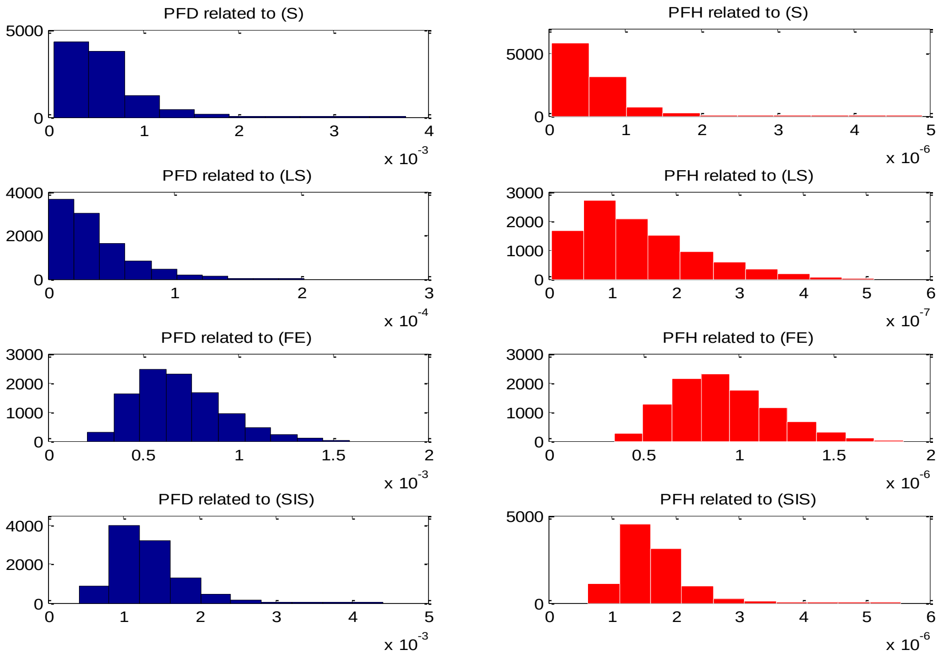


Fig. 5.9 Histograms related to PFD_{avg} and PFH for S, LS, FE and SIS

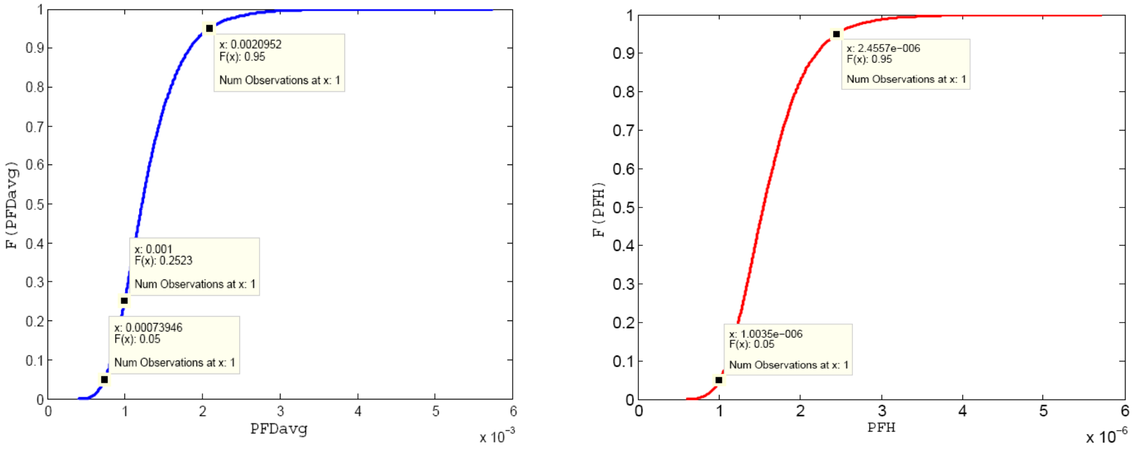


Fig. 5.10 Cumulative distribution function of PFD_{avg} and PFH

According to the results of Table 5.16, the SIS can provide a safety function with SIL 2 in the low demand mode and SIL 1 in high demand mode. These assignments are valid with probabilities higher than 95 % since $p(X \leq 10^{-2}) = 1$ for PFD_{avg} and $p(\mathrm{X} \leq 10^{-5}) = 1$ for PFH.

At this point we take the same SIS and we assume that its related reliability characteristics are those gathered in Table 5.17. Using the fuzzy sets' principles and relations, we can obtain the results of Fig. 5.11, and Table 5.18.

Table 5.17 Fuzzy characteristics for the SIS elements

Parameters	**Subsystem S:** **1oo3**	**Subsystem LS:** **1oo2**	**Subsystem FE:** **2oo5**
$\boldsymbol{\lambda_D}$ (h^{-1})	(1.48E–6, 4.35E–6, 9.26E–6)	(5E–7, 3.67E–6, 1E–5)	(3E–6, 5.33E–6, 1E–5)
DC	(0.6, 0.7, 0.8)	(0.95, 0.97, 0.99)	(0.2, 0.3, 0.4, 0.5)
$\boldsymbol{\beta}$	(0.15, 0.2, 0.25, 0.3)	(0.01, 0.055, 0.1)	(0.1, 0.15, 0.2)
$\boldsymbol{\beta_D}$	(0.07, 0.1, 0.15)	(0.005, 0.0275, 0.05)	(0.1, 0.15 ,0.2)
MTTR & MRT (h)	(8, 12 ,16)	(5, 9, 15)	(8, 18, 30)
$\boldsymbol{T_1}$ (h)	4380	8760	2190

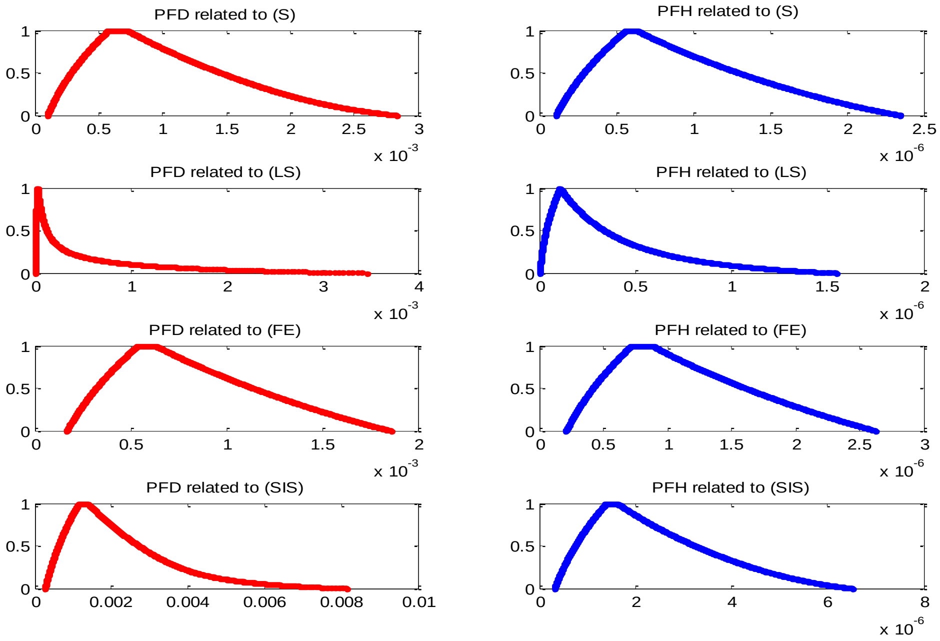


Fig. 5.11 Fuzzy numbers related to PFD_{avg} and PFH for S, LS, FE and SIS

Table 5.18 Obtained results from the fuzzy sets approach ($d\alpha$ =1E-3)

Elements	$\boldsymbol{PFD_{avg}}$ ***(COG)***			***PFH (COG)*** (h^{-1})	
S	1.0E–3			9.327E–7	
LS	6.920E–4			3.792E–7	
FE	8.182E–4			1.138E–6	
SIS	2.30E–3			2.418E–6	
	α	$\boldsymbol{PFD_L^{(\alpha)}}$	$\boldsymbol{PFD_R^{(\alpha)}}$	$\boldsymbol{PFH_L^{(\alpha)}}$	$\boldsymbol{PFH_R^{(\alpha)}}$
	0.0	3.0E–4	8.2E–3	3.19E–7	6.52E–6
	0.1	3.0E–4	5.1E–3	3.86E–7	5.43E–6
	0.2	4.0E–4	4.1E–3	4.62E–7	4.72E–6
	0.3	4.0E–4	3.5E–3	5.46E–7	4.15E–6
	0.4	5.0E–4	3.1E–3	6.38E–7	3.67E–6
	0.5	6.0E–4	2.7E–3	7.39E–7	3.25E–6
	0.6	7.0E–4	2.4E–3	8.50E–7	2.86E–6
	0.7	8.0E–4	2.1E–3	9.70E–7	2.51E–6
	0.8	9.0E–4	1.8E–3	1.10E–6	2.19E–6
	0.9	1.0E–3	1.6E–3	1.24E–6	1.89E–6
	1.0	1.1E–3	1.4E–3	1.39E–6	1.62E–6

Obviously, the resulted uncertainty is somewhat bigger than that obtained using MC simulation: $PFD_{avg}^{(\alpha=0)}$= [3.0E-4, 8.2E-3] and $PFH^{(\alpha=0)}$= [3.19E-7, 6.52E-6]. However, the 1-cuts are close to the mean values given by MC simulation: $PFD_{avg}^{(\alpha=1)}$= [1.1E-3, 1.4E-3] and $PFH^{(\alpha=1)}$= [1.39E–6, 1.62E–6]. 1-cuts mean that the corresponding intervals belong to the fuzzy number of interest (PFD_{avg} or *PFH*) with confidence of 100 %. The crisp values derived using the centroid (COG) method are: PFD_{avg}^{COG}= 2.3E-3 and PFH^{COG}= 2.418E-6 h^{-1}. Although these values are higher than those derived from MC simulation, they provide the same SILs for both demand modes. Furthermore, if one uses the method of the largest of maximum (maximum values of 1-cuts intervals), the obtained crisp values for PFD_{avg} and *PFH* will be respectively 1.4E–3 and 1.62E–6 h^{-1}. These latter are very close to those resulted from MC simulation, which are respectively 1.299E-3 and 1.619E-6 h^{-1}. Actually, these latter conclusions cannot be generalized and the method of the largest of maximum is not conservative and does not take into account the variation of the whole fuzzy number. Thus, the COG is preferred in spite of the fact that it gives a conservative value (which is safer).

As required by the route 2_H, the mean value is not sufficient to identify the claimed SIL for the safety function. So the whole fuzzy number has to be compared with the compliance criteria (SIL_{RU} or a specified target). It is clear that the possibility to reach the range of variation defined by the 0-cut is very low. On the other hand, 1-cut intervals do not take into account different values with high degree of membership (0.9, 0.8, etc.). To handle this problematic situation, the analyst may choose an arbitrary interval with for example α = 0.6 and compare the upper limit of that interval to the upper limit of the required SIL zone (SIL_{RU}). However, what value for α should be chosen? In what follows, we propose two ways in order to avoid any extra uncertainty due to the choice of α.

- **Possibility and necessity measures**

In order to compare the resulted fuzzy numbers (PFD_{avg} or *PFH*) with the SIL_{RU} value, the theory of possibility offers two measures: *possibility* (Π) and *necessity* (N). In our case, these two measures are used to evaluate the proposition "PFD_{avg} (or *PFH*) is lower than or equal to SIL_{RU}". From this latter, we can identify two fuzzy sub-sets: "*A* =PFD_{avg} (or *PFH*)" and "*B* = lower than or equal to SIL_{RU}". The possibility and necessity measures are defined as follows:

$$\begin{cases}\Pi(A \text{ is } B) = \Pi(B, A) = \text{Sup}_x \min\{\mu_A(x),\ \mu_B(x)\} \\ \text{N}(A \text{ is } B) = \text{N}(B, A) = \text{Inf}_x \max\{1-\mu_A(x),\ \mu_B(x)\}\end{cases} \tag{5.12}$$

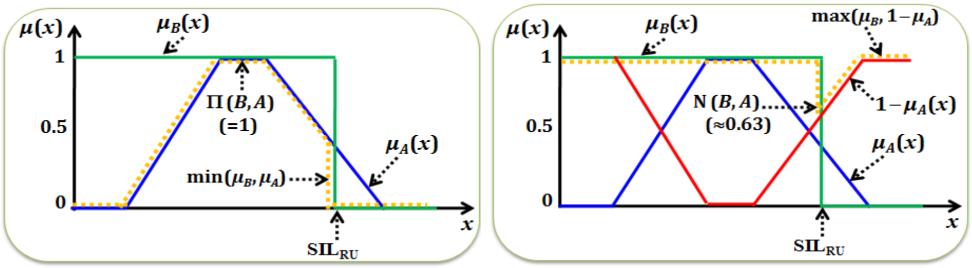


Fig. 5.12 Possibility and necessity measures for a given $\mathrm{SIL_{RU}}$

From Fig. 5.12, we can observe that $\Pi(A \text{ is } B)$ is given by the height of the intersection of the two fuzzy sub-sets. In some way, $\Pi(A \text{ is } B)$ measures the maximum extent to which an element x belongs to both A and B. $\mathrm{N}(A \text{ is } B)$ determines the degree to which A is included in B. $\Pi(A \text{ is } B)$ and $\mathrm{N}(A \text{ is } B)$ may be interpreted as upper and lower bounds for the probability that $(A \text{ is } B)$, i.e., that the obtained fuzzy number is lower than or equal to $\mathrm{SIL_{RU}}$. Therefore, it appears that only the necessity measure can be useful for decision making process, even if it could be pessimistic. One may, for example, set a tolerable necessity measure at 0.9.

- **Fuzzy number compliance probability**

This second way based on the following equation:

$$p_F(A \leq SIL_{RU}) = \frac{\int_{x \leq \mathrm{SIL_{RU}}} \mu_A(x)\mathrm{d}x}{\int_x \mu_A(x)\mathrm{d}x} \qquad (5.13)$$

where $p_F(A \leq SIL_{RU})$ expresses the compliance probability of the fuzzy number A (PFD_{avg} or PFH) with the required SIL (see Fig. 5.13).

The following table shows the results of applying Eq. (5.13) for the preceding example. For comparison purposes, the results obtained from MC simulation are also reported.

Table 5.19 Compliance measures related to different required SILs

Required SIL			***Fuzzy sets***						***MC***	
SIL	$\mathrm{SIL_{RU}}$		Π	N	Π	N	$p_F(A \leq \mathrm{SIL_{RU}})$		$p(X \leq \mathrm{SIL_{RU}})$	
	PFD	*PFH*	*PFD*	*PFD*	*PFH*	*PFH*	*PFD*	*PFH*	*PFD*	*PFH*
SIL 1	1E–1	1E–5	1	1	1	1	1	1	1	1
SIL 2	1E–2	1E–6	1	1	0.724	0	1	0.102	1	0.049
SIL 3	1E–3	1E–7	0.884	0	0	0	0.151	0	0.252	0
SIL 4	1E–4	1E–8	0	0	0	0	0	0	0.00	0

We can conclude that the proposed compliance measures, pertaining to MC simulation and fuzzy sets approaches provide the same maximum claimed SIL: SIL 2 for the low demand mode and SIL 1 for the high demand mode. Also, the necessity measure is systematically lower than p_F.

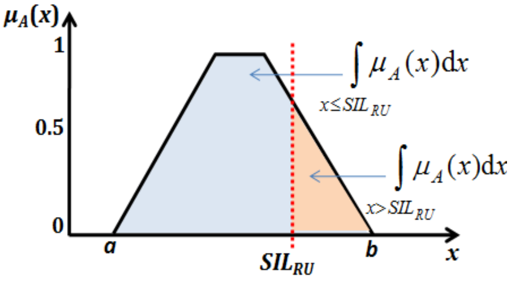


Fig. 5.13 Compliance probability principle

We propose here a new method to handle the diversity in the nature of the involved data thorough the combination of MC simulation and fuzzy sets. Fig. 5.14 shows its overall process which is described hereafter. This process is fully automated within a computer code developed under the MATLAB (MATLAB, 2009) environment.

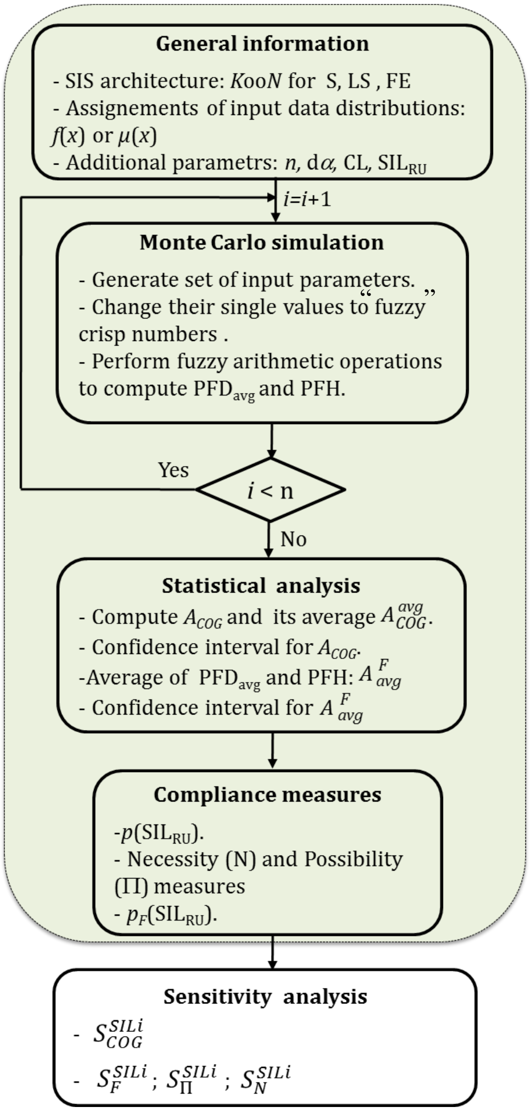

General information
- SIS architecture: *KooN* for S, LS , FE
- Assignements of input data distributions: $f(x)$ or $\mu(x)$
- Additional parametrs: n, dα, CL, $\mathrm{SIL_{RU}}$
i=i+1
Monte Carlo simulation
- Generate set of input parameters.
- Change their single values to "fuzzy" crisp numbers .
- Perform fuzzy arithmetic operations to compute $\mathrm{PFD_{avg}}$ and PFH.
Yes
i < n
No
Statistical analysis
- Compute A_{COG} and its average A^{avg}_{COG}.
- Confidence interval for A_{COG}.
-Average of $\mathrm{PFD_{avg}}$ and PFH: A^F_{avg}
- Confidence interval for A^F_{avg}
Compliance measures
-$p(\mathrm{SIL_{RU}})$.
- Necessity (N) and Possibility (Π) measures
- $p_F(\mathrm{SIL_{RU}})$.
Sensitivity analysis
- S^{SILi}_{COG}
- S^{SILi}_{F} ; S^{SILi}_{Π} ; S^{SILi}_{N}

Fig. 5.14 Overall process for combining MC and fuzzy sets

5.4.1 General information

The first step of the proposed method is the assignment of all the input data, including K and N of the three subsystems of the SIS, probability distributions and/or membership functions of the uncertain parameters. Several probability distributions are implemented, namely: Uniform, Triangular, Normal, Lognormal, Chi-square, Beta and Gamma. The constant law is represented as a fuzzy number in order to easily handle the fuzzy representations: crisp value a = [a, a, a, a]. Also, the Triangular and Trapezoidal fuzzy numbers are considered. Additional inputs are also required such as n (number of MC iterations), required SIL upper bounds ($\mathrm{SIL}_{\mathrm{RU}}$) for PFD_{avg} and PFH, confidence level (CL) (to compute confidence intervals) and the increment of the α-cuts ($d\alpha$).

5.4.2 Monte Carlo simulation

The main idea of the proposed procedure is MC simulation driven by fuzzy arithmetic. In fact, if at least one parameter is represented by a fuzzy number, all the resulted amounts are also fuzzy numbers. Once the first step is fulfilled, a MC sampling is performed for the assigned pdfs. To deal with uncertainties specified as fuzzy numbers, each input parameter issued from the sampling is changed to a crisp number a = [a, a, a, a]. Hence, arithmetic operations may take place to evaluate PFD_{avg} and PFH, of course they are expressed as fuzzy numbers and entirely defined by their α-cuts. At the end of this step, the results are stored in two matrices for PFD_{avg} and PFH, where each row represents the obtained value for the corresponding iteration (A stands for PFD_{avg} or PFH):

$$A = \begin{bmatrix} A_{L_1}^{(\alpha_1=0)}, \dots, A_{L_1}^{\left(\alpha_{\left(\frac{1}{d\alpha}\right)+1}=1\right)}, & A_{R_1}^{\left(\alpha_{\left(\frac{1}{d\alpha}\right)+2}=1\right)}, \dots, A_{R_1}^{\left(\alpha_{2\left(\frac{1}{d\alpha}\right)+2}=0\right)} \\ & \vdots \\ A_{L_n}^{(\alpha_1=0)}, \dots, A_{L_n}^{\left(\alpha_{\left(\frac{1}{d\alpha}\right)+1}=1\right)}, & A_{R_n}^{\left(\alpha_{\left(\frac{1}{d\alpha}\right)+2}=1\right)}, \dots, A_{R_n}^{\left(\alpha_{2\left(\frac{1}{d\alpha}\right)+2}=0\right)} \end{bmatrix} \tag{5.14}$$

5.4.3 Statistical analysis

The first computed metrics is the COG of each fuzzy number (each row of the matrices). The average of the obtained COGs can be obtained as follows:

$$A_{COG}^{avg} = \frac{1}{n} \cdot \sum_{i=1}^{n} A_{COG}^{i} \tag{5.15}$$

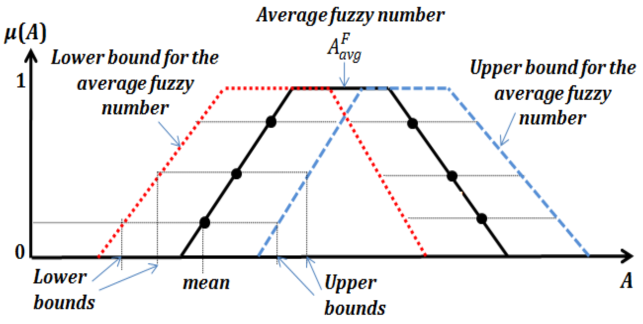
In addition, the confidence interval of A_{COG}^{avg} at a given level (CL) is obtained from its CDF: $\left[A_{COG\left(\frac{1-CL}{2}\right)}, A_{COG\left(\frac{1+CL}{2}\right)}\right] = \left[A_{COG_L}, A_{COG_U}\right]$, where:

$$\begin{cases} p\left(A_{COG} \leq A_{COG\left(\frac{1-CL}{2}\right)}\right) = \frac{1-CL}{2} \\ p\left(A_{COG} \leq A_{COG\left(\frac{1+CL}{2}\right)}\right) = \frac{1+CL}{2} \end{cases} \tag{5.16}$$

Also, from Eq. (5.14), we can obtain the average fuzzy number by using the following equation:

$$A_{avg}^{F} = \left[\frac{\sum_{i=1}^{n} A_{L_i}^{(\alpha_1=0)}}{n}, \dots, \frac{\sum_{i=1}^{n} A_{L_i}^{\left(\alpha_{\left(\frac{1}{d\alpha}\right)+1}=1\right)}}{n}, \frac{\sum_{i=1}^{n} A_{R_i}^{\left(\alpha_{\left(\frac{1}{d\alpha}\right)+2}=1\right)}}{n}, \dots, \frac{\sum_{i=1}^{n} A_{R_i}^{\left(\alpha_{2\left(\frac{1}{d\alpha}\right)+2}=0\right)}}{n}\right] \tag{5.17}$$

We try now to establish a confidence interval for the resulted average fuzzy number: upper (A_U^F) and lower (A_L^F) bounds, which are also fuzzy numbers. We know that the elements associated with each column of the matrix A have a pdf. Thus, each column may be characterized by a mean (given by Eq. (5.17)), lower and upper bounds computed at a given confidence level (CL). By doing so, the upper bound (or lower bound) of the confidence interval for the average fuzzy number A_{avg}^Fcould be specified by these individual upper bounds (or lower bounds), see Fig. 5.15. Their corresponding COGs are respectively noted $A_{COG_{\mathrm{U}}}^F$and $A_{COG_{\mathrm{L}}}^F$.



Average fuzzy number
A_{avg}^F
$\mu(A)$
Lower bound for the average fuzzy number
Upper bound for the average fuzzy number
1
0
Lower bounds
mean
Upper bounds
A

Fig. 5.15 Confidence interval for the average fuzzy number

5.4.4 Compliance measures

All the compliance measures already presented are computed:

- ✓ $p(A_{\mathrm{COG}} \leq \mathrm{SIL_{RU}})$ derived from the empirical CDF of the COGs
- ✓ $p_F\,(A_{avg}^F \leq \mathrm{SIL_{RU}})$ computed according to Eq. (5.13)
- ✓ Possibility and necessity measures given by Eq. (5.12), where the proposition A represents here the average fuzzy number A_{avg}^F

5.4.5 Sensitivity analysis

We identify here some sensitivity indicators.

Based on the distribution of A_{COG}, we consider the following indicator:

$$S_{COG}^{(SIL)} = p\left(A_{COG}^{(x)} \leq SIL_{RU}\right) - p(A_{COG} \leq SIL_{RU}) \tag{5.18}$$

where $A_{COG}^{(x)}$ is the distribution of A_{COG} without taking into consideration the uncertainty of the parameter x. Actually, $S_{COG}^{(SIL)}$may be positive or negative, according to SIL$_{\text{RU}}$ and the shift direction of A_{COG} distribution. A positive value indicates the increase amount of $p(A_{COG} \leq SIL_{RU})$ due to the elimination of uncertainty related to x. Hence, the positive $S_{COG}^{(SIL)}$ gives an idea about the parameters which would lead to an optimistic achievable SIL (which is dangerous) when their related uncertainties are not considered. In contrast, a negative value indicates the decreasing of that probability. Thus, the negative $S_{COG}^{(SIL)}$ shows the parameters that can produce a pessimistic result for the achievable SIL (which is safer) when their associated uncertainties are not considered.

With respect to the previous conclusions, the ranking rule is: the higher the indicator is, the more influential the parameter on the uncertainty of the output with regard to the required SIL.

In the case of considering the average fuzzy number (A_{avg}^{F}), we propose to use the following three measures:

The first sensitivity indicator (noted S_{F}^{SIL}) is defined by Eq. (5.19). It evaluates the impact of the parameter's uncertainty on the output expressed by a fuzzy number, with respect to the required SIL.

$$S_{F}^{(SIL)} = p_F\left(A_{avg}^{F(x)} \leq SIL_{RU}\right) - \ p_F\left(A_{avg}^{F} \leq SIL_{RU}\right) \tag{5.19}$$

The other two indicators are based on the variation of the possibility (Π) and necessity (N) measures:

$$S_{\Pi}^{(SIL)} = \ \Pi\left(A_{avg}^{F(x)} \leq SIL_{RU}\right) - \Pi\left(A_{avg}^{F} \leq SIL_{RU}\right) \tag{5.20}$$

$$S_{N}^{(SIL)} = \ \mathrm{N}\left(A_{avg}^{F(x)} \leq SIL_{RU}\right) - \mathrm{N}\left(A_{avg}^{F} \leq SIL_{RU}\right) \tag{5.21}$$

By eliminating the uncertainty of the parameter x, the compliance probability, possibility and necessity measures of the new average fuzzy number $A_{avg}^{F(x)}$ increase or decrease according to the SIL$_{\text{RU}}$ value. Thus, all conclusions made for $S_{COG}^{(SIL)}$ still applicable for these last ones.

5.4.6 Illustrative example

In order to illustrate the application of the proposed procedure, let us consider a SIS with the reliability characteristics of Table 5.20. The obtained results are presented in Table 5.21, while Fig. 5.16 depicts the average fuzzy numbers (*PFD$_{avg}$* and *PFH*) corresponding to the SIS and its subsystems. Fig. 5.17 represents the COGs histograms and CDFs related to the SIS's *PFD$_{avg}$* and *PFH*, while Fig. 5.18 maps the confidence intervals of the SIS's average fuzzy numbers.

Table 5.20 Reliability characteristics for the SIS elements

Parameters	**Subsystem S:**	**Subsystem LS:**	**Subsystem FE:**
	1oo3	**1oo2**	**2oo5**
$\boldsymbol{\lambda_D}$ (h^{-1})	Logn. (–12.5, 0.557)	(5E–7, 3.67E–6, 1E–5)	Trian. (3E–6, 1E–5, 5.33E–6)
DC	(0.6, 0.7, 0.8)	(0.95, 0.97, 0.99)	(0.2, 0.3, 0.4, 0.5)
$\boldsymbol{\beta}$	(0.15, 0.2, 0.25, 0.3)	(0.01, 0.055, 0.1)	(0.1, 0.15, 0.2)
$\boldsymbol{\beta_{\mathrm{D}}}$	Gam. (3.70, 0.027)	(0.005, 0.0275, 0.05)	(0.1, 0.15 ,0.2)
MTTR & MRT(h)	Logn. (2.43, 0.21)	Logn. (2.047, 0.4)	Logn. (2.85, 0.34)
$\boldsymbol{T_1}$ (h)	Constant (4380)	Constant (8760)	Constant (2190)

Table 5.21 Obtained results from the combined approach

n = 10000; dα = 0.001and CL= 90%		
Metrics	$\boldsymbol{PFD_{avg}}$	***PFH*** (h^{-1})
A_{COG}^{avg}	Mean = 2.41E–3	Mean = 1.91E–6
	σ = 8.18E–4	σ = 4.70E–7
$\left[A_{COG_{\mathrm{L}}}, A_{COG_{\mathrm{U}}}\right]$	[1.5E–3, 3.9E–3]	[1.3E–6, 2.7E–6]
A_{COG}^{F}	2.41E–3	1.91E–6
$\left[A_{COG_{\mathrm{L}}}^{F}, A_{COG_{\mathrm{L}}}^{F}\right]$	[1.5E–3, 3.9E–3]	[1.3E–6, 2.8E–6]
$p\,(A_{COG} \leq \mathrm{SIL_{RU}})$	$p(\,A_{COG} \leq$ 1E–2) = 1 $p(\,A_{COG} \leq$ 1E–3) = 0	$p(\,A_{COG} \leq$ 1E–5) = 1 $p(\,A_{COG} \leq$ 1E–6) = 1E-4
$p_F\,(A_{avg}^{F} \leq \mathrm{SIL_{RU}})$	$p_F(A_{avg}^{F} \leq$ 1E–2) = 1	$p_F(A_{avg}^{F} \leq$ 1E–5) = 1
	$p_F(A_{avg}^{F} \leq$ 1E–3) = 2.6E–3	$p_F(A_{avg}^{F} \leq$ 1E–6) = 2.2E–2
$\Pi\,(A_{avg}^{F} \leq \mathrm{SIL_{RU}})$	$\Pi(A_{avg}^{F} \leq$ 1E–2) = 1	$\Pi(A_{avg}^{F} \leq$ 1E–5) = 1
	$\Pi(A_{avg}^{F} \leq$ 1E–3) = 1.1E–1	$\Pi(A_{avg}^{F} \leq$ 1E–6) = 3.2E–1
$N\,(A_{avg}^{F} \leq \mathrm{SIL_{RU}})$	$N(A_{avg}^{F} \leq$ 1E–2) = 1	$N(A_{avg}^{F} \leq$ 1E–5) = 1
	$N(A_{avg}^{F} \leq$ 1E–3) = 0	$N(A_{avg}^{F} \leq$ 1E–6) = 0

The mean value of A_{COG}^{avg} and A_{COG}^{F} show that the studied SIS can provide safety functions with SIL 2 in the low demand mode and SIL 1 in the high and/or continuous demand modes. Obviously, the obtained SILs are the same in the case of employing MC simulation and fuzzy analysis separately, the matter that could not be the same in other applications. Also, we can conclude that A_{COG}^{avg} and A_{COG}^{F} are almost identical, whatever the value of n (MC runs) is. The confidence in those claimed SILs is evaluated according to the four suggested compliance measures, where all of them provide the same confidence (100%) in the cases where $\mathrm{SIL_{RU}}$=1E–2 for PFD_{avg} and $\mathrm{SIL_{RU}}$=1E–5 for PFH.

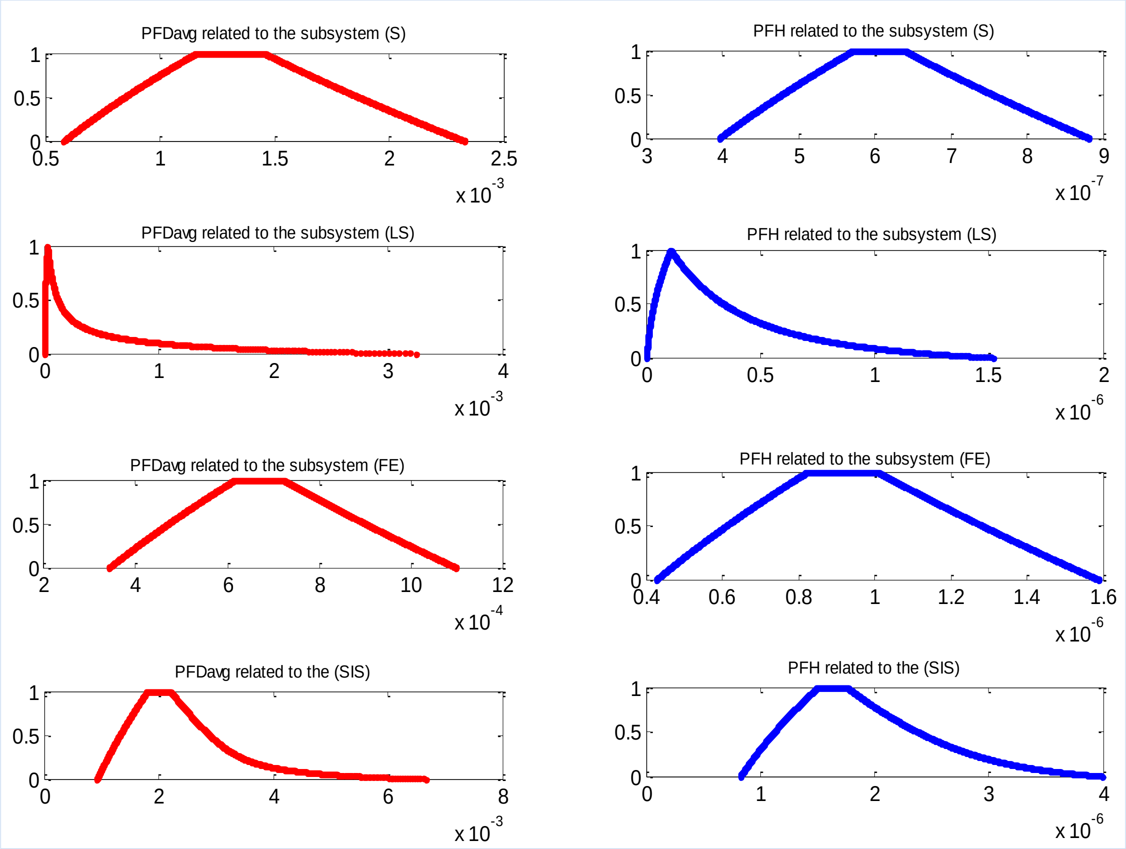


Fig. 5.16 Average fuzzy numbers related to PFD_{avg} and *PFH*

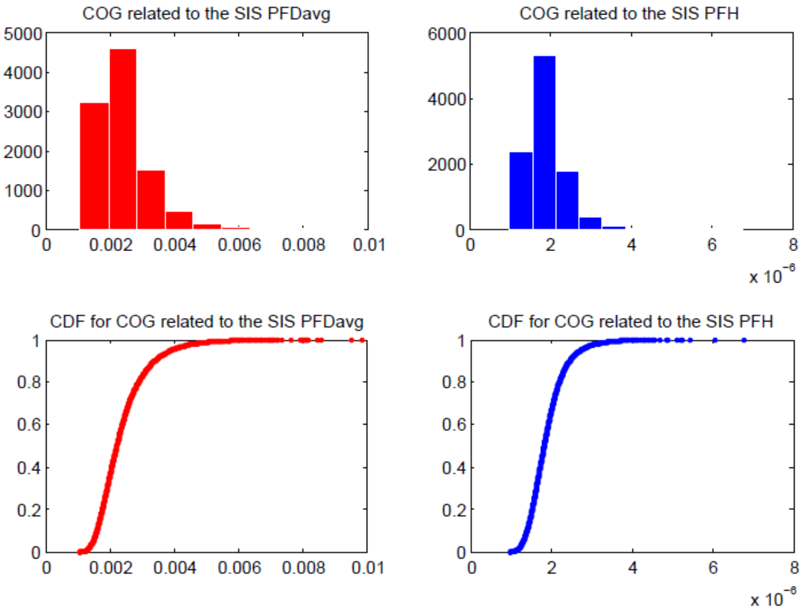


Fig. 5.17 Histograms and CDFs for COGs related to the SIS PFD_{avg} and *PFH*

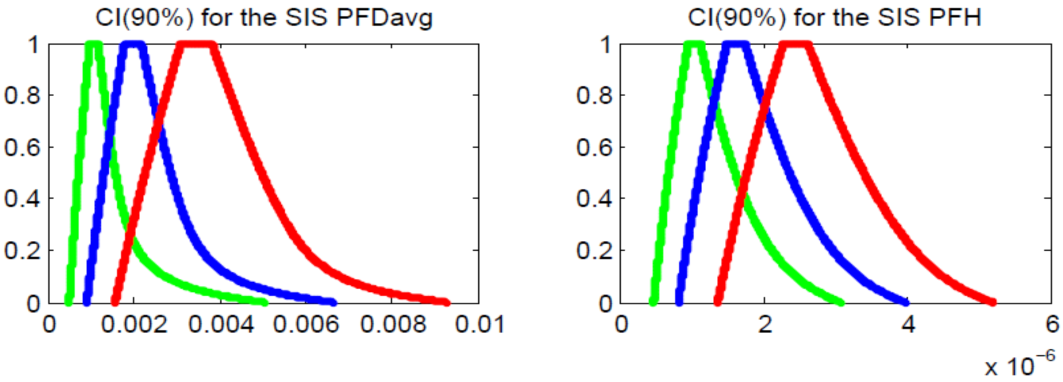


Fig. 5.18 The SIS's PFD_{avg} and PFH confidence intervals

Table 5.22 provides the results of the sensitivity analysis associated with the parameters λ_D, DC, β and β_D used for FE subsystem.

Table 5.22 Sensitivity measures related to the parameters of the subsystem FE

x **(*FE*)**	$\boldsymbol{PFD_{avg}}$				***PFH***			
	$S_{COG}^{(SIL2)}$	$S_{F}^{(SIL2)}$	$S_{\Pi}^{(SIL2)}$	$S_{N}^{(SIL2)}$	$S_{COG}^{(SIL1)}$	$S_{F}^{(SIL1)}$	$S_{\Pi}^{(SIL1)}$	$S_{N}^{(SIL1)}$
$\boldsymbol{\lambda_D}$	0.0 **2**	-4.73E-5 **2**	-1.00E–3 **2**	0.0	-1.0E-4 **3**	-7.13E-4 **1**	-5.00E-3 **1**	0.0
DC	1.0E-4 **1**	-2.59E-3 **3**	-1.11E–1 **3**	0.0	5.0E-4 **1**	-2.19E-2 **4**	-3.19E-1 **4**	0.0
$\boldsymbol{\beta}$	0,0 **2**	-2.59E-3 **3**	-1.11E–1 **3**	0.0	4.0E-4 **2**	-2.12E-2 **3**	-2.54E-1 **3**	0.0
$\boldsymbol{\beta_D}$	0,0 **2**	1.43E-4 **1**	3.00E–3 **1**	0.0	4.0E-4 **2**	-1.05E-2 **2**	-8.60E-2 **2**	0.0

From this latter table we can notice that: according to $S_{COG}^{(SIL)}$, PFD_{avg} and PFH are primarily sensitive to DC. Obviously, this sensitivity measure gives the same parameters' ranking for both performance indicators. On the other hand, $S_{F}^{(SIL)}$ and $S_{\Pi}^{(SIL)}$, which are based on the average fuzzy number, give the same parameters' ranking (but different between PFD_{avg} and PFH).

Despite the fact that $S_{F}^{(SIL)}$ and $S_{\Pi}^{(SIL)}$ produce different rankings compared to that given by $S_{COG}^{(SIL)}$, all of them indicate the insignificant change on the compliance measures with and without considering the uncertainties, which is more apparent in the case of $S_{N}^{(SIL)}$ designating that the two outputs are almost insensitive to the input parameters' uncertainties.

5.5 Conclusion

Since they form the prime foundation upon which several decisions must be taken that have a forthright impact on humans' safety, environment, etc., the importance of the various SISs performance indicators is downright. Such importance requires the prudent and best possible assessment of those indicators. Uncertainty analysis is one of the aspects that are considered substantial in most of the modeling processes. Indeed, several types and forms of uncertainty are involved in the context of SISs, while explicit borders between them are often absent. However, the principal objective of this chapter was the handling of the parameter uncertainty, which is associated with data to be used for feeding the involved models. In the literature, several methods and tools have been proposed to deal with this type of uncertainties, which can deeply differ from each other.

One of the main focuses in this chapter was the choice of the method that can be employed to address the parametric uncertainties associated with the estimation of PFD_{avg} and PFH and even the other performance indicators, including the operational integrity ones. Clearly, the first criterion to be considered in the selection of the appropriate method is the data's nature and quality, where no important information and properties should be wasted, avoid the overestimations, no unneeded and misleading assumptions must be taken, and even no unnecessary efforts should be paid where it is not required. Another decisive factor is the consideration of the nature of the models that are commonly and practically utilized to estimate the different performance metrics of SIS, since it's not cogent to ask the addition of an extra complexity on the methods that are already not employed because of their intricacies.

In order to handle the parametric uncertainty in the context of SIS, many methods and techniques have been appointed, adapted and even combined in this chapter, namely: MC simulation, ENs, PBA and fuzzy sets analysis, where each one has its own specificity and domain of applicability. Actually, it seems that the IEC 61508 requirement regarding the consideration of uncertainties in the estimation of PFD_{avg} and PFH should be generalized by implementing it no matter what route is selected (1_H or 2_H), since the ignorance of such task can violate the key role of those estimates. Although, the concentration in the case studies was on the performance indicators of safety integrity, the same ways can be used in the same manner for the ones of operational integrity.

Sensitivity analysis has been addressed within different frameworks using multiple measures. Often, those alternatives agree only when there is a certain difference in terms of the amount of uncertainty between the various variables. However, as pointed out earlier, it is very beneficial to know which input parameter is contributing the most in the generated uncertainty and the nature of that contribution.

Conclusions and perspectives

Relying on the importance of the realization phase on the whole safety lifecycle, the main purpose of this study is to provide a new framework for modeling the performance of SISs in terms of safety integrity and operational integrity, where the focus is on making the results of such process: a) as simple as possible to facilitate the task of the user and minimize the chances of mistaking, and b) as authentic as possible through the appropriate treatment of the related uncertainties that have a great potential to change the direction of the ultimate decisions that are based on such results.

By proposing a unified approach based on Markov chains to deal with the various parametric models which were created to handle the CCF events, it has been proven that the widespread thought on the conservative character of Beta Factor model is only true when the value of K of any $KooN$ architecture is equal to one. Additionally, the comparison of the Beta Factor and MBF models has demonstrated that increasing the value of β_2 does not necessarily lead to making the MBF model closer to the BF one.

Furthermore, for the configurations whose diagnostic devices have not the capability to de-energize the associated output, it has been shown in the comparative study that included large variations in the values of all of the failure rates, diagnostic coverage and β factors that: a) the ignorance of the contribution of safe failures in the estimation of both PFD_{avg} and PFH has no adverse effects on the safety integrity, and b) the elimination of the dangerous failures in the evaluation of the operational integrity's measures can cause a slight overestimation in the results. These last remarks could be taken into consideration while trying to find a compromise between safety integrity and operational integrity.

New generalized formulas have been developed for the two safety integrity's metrics PFD_{avg} and PFH in the fourth chapter. In addition to their important simplicity, the proposed models can simultaneously take into account the contributions of all of the dangerous detected and undetected failures, partial stroking and proof testing, and CCF events, while their adaptation to the various situations and scenarios can smoothly be carried out. The validity of the obtained analytical expressions is ensured at different levels of their construction through the various comparisons that are implemented between the results they yield with the ones of some of the accepted methods. In the same chapter, a new formulation for the analytical expressions of the operational integrity's measures PFS_{avg} and STR has been conducted. This new formulation is based on the use of the corresponding generalized and approximated Markov model. Once again, the results of those formulas were compared to the ones obtained via the corresponding multi-phase Markov models and Faults trees.

Several types of uncertainty are involved in the estimation of the various performance indicators of SISs. Parametric uncertainty is associated with the values of the input parameters that should be used to quantify such indicators. The functional safety-related standard IEC 61508 requires the treatment of this type of uncertainty in the evaluation of PFD_{avg} and PFH when Route 2_H is selected. Definitely, there are many frameworks for the treatment of the parametric uncertainties and the disagreement about the most appropriate one is always present. However, each approach has its own domain of application that depends on the nature of the related parameters and data. For the assessment of both sides of performance of SISs, we have considered three different scenarios, namely: a) enough information for assigning precise pdfs for all the input parameters, b) the only available information about the values of each parameter is provided as a simple interval, and c) different types of data are involved. Actually, this latter case can be considered as the most encountered one in practice, where the intervention of a hybrid approach seems to be the best solution to deal with such variety in the types of the concerned data. In our case, we have employed the PBA that showed an important degree of flexibility and adequacy for the treatment of the parametric uncertainty in the context of SISs. Additionally, an alternative approach based on the combination of MC simulation and fuzzy sets theory has been proposed to deal with such case. Diverse methods and measures have been used to analyze the sensitivity of the outputs to each input parameter's uncertainty, which is a quite advantageous task to figure out if there is any benefit from the further research and collection, and where should be the focus.

Many interesting points can be treated in future research. For instance, it is highly recommended to apply the suggested unified Markov model using the BFR model and maybe compare the obtained results with the ones of the other parametric models, especially the traditional Beta Factor model. The unified Markov model itself can be improved by incorporating other failure modes and repair policies then why not extract from it generalized formulas for the different performance indicators that can take into account any parametric model. Certainly, there is always a scope and need to improve the generalized analytical formulas of the different performance indicators by exploring several ideas and properties to add more simplicity and/or to integrate the contribution of many other factors. The treatment of both uncertainty and sensitivity represents a fertile and tricky ground at the same time. However, the focus on the hybrid approaches is advantageous and the management of the model and completeness uncertainties is very beneficial.

References

29 CFR1910.119 Process Safety Management of Highly Hazardous Chemicals // Occupational Safety and Health Administration. - Washington, DC : U.S. Department of Labor , 1992.

ANSI / API RP-754 Process Safety Performance Indicators for the Refining and Petrochemical Industries. - Washington D.C : American Petroleum Institute, 2010.

ANSI/ISA-84.00.01-2004 Functional Safety: Safety Instrumented Systems for the Process Industry Sector. - NC : ISA, 2004.

ANSI/ISA-84.01-1996 Application of Safety Instrumented Systems for the Process Industries. - NC : Research Triangle Park, ISA, 1996.

ANSI/ISA-TR96.05.01 Partial Stroke Testing of Automated Block Valves. The International Society of Automation, 2008.

API Guide to Reporting Process Safety Events (Version 2.0). American Petroleum Institute.

Apostolakis G E Uncertainty in Probabilistic Safety Assessment [Journal] // Nuclear Engineering and Design. - 1989. - Vol. 115. - pp. 173-179.

ASME/ANS Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications. ASME/American Nuclear Society, 2009.

Aughenbaugh Jason Matthew and Paredis Christiaan J J Probability Bounds Analysis as a General Approach to Sensitivity Analysis in Decision Making Under Uncertainty. - 2007.

Avizienis Algirda and Laprie Jean-Claud Dependable Computing: From Concepts to Design Diversity [Journal] // Proceedings of the IEEE. IEEE , 1986. - 5 : Vol. 74. - pp. 629 - 638.

Avizienis Algirdas, Laprie Jean Claude and Randell Brian Basic Concepts and Taxonomy of Dependable and Secure Computing [Journal] // IEEE Transactions on Dependable and Secure Computing. - 2004. - 1 : Vol. 1. - pp. 11 - 33.

Avizienis Algirdas, Laprie Jean Claude and Randell Brian Fundamental Concepts of Dependability [Conference] // Proceedings of the 3rd IEEE Information Survivability Workshop. - Boston : IEEE, 2000. - pp. 7-12.

Baker III James A, Bowman Frank L, Erwin Glenn, Gorton Slade, Hendershot Dennis, Leveson Nancy, Priest Sharon, Rosentha Isadorel, Tebo Paul V, Wiegmann Douglas A and Wilson L Duane The Report of the BP U.S. Refineries Independent Safety Review Panel. - 2007.

Baradits György, Madár János and Abonyi János Novel Model of Proof Test Coverage Factor [Conference] // 10th International Symposium of Hungarian Researchers on Computational Intelligence and Informatics. - Budapest, 2009.

Barner Andreas, Bredau Jan and Schiller Frank Efficient Drive-Based Analysis of Fault Detection Measures in Safety-Related Pneumatic Systems [Conference] // 21st International Workshop on Principles of Diagnosis. - Portland, 2010.

Baudrit Cédric Représentation et Propagation de Connaissances Imprécises et Incertaines : Application à l'évaluation des Risques Liés aux Sites et aux Sols Pollués [Ph.D dissertation]. Université Toulouse III - Paul Sabatier, 2005.

Berleant Daniel and Goodman-Strauss Chaim Bounding the Results of Arithmetic Operations on Random Variables of Unknown Dependency Using Intervals [Journal] // Reliable Computing. - 1998. - 2 : Vol. 4. - pp. 147-165 .

Berleant Daniel Automatically Verified Reasoning with Both Intervals and Probability Density Functions [Journal] // Interval Computations. - 1993. - Vol. 2. - pp. 48-70.

Birnbaum Z W On the Importance of Different Components in a Multicomponent System [Journal] // Journal of Multivariate Analysis. - 1969.

Borcsok J, Holub P and Machmur D Probability of Failure on Demand for Systems with Partial Stroke Test [Journal] // International Journal of Mathematical Models and Methods in Applied Sciences . - 2007. - 4 : Vol. 1.

BP British Petroleum Energy Outlook 2035. - 2014. - http://www.bp.com/content/dam/bp/pdf/Energy-economics/Energy-Outlook/Energy_Outlook_2035_booklet.pdf.

Bridges William G The Cost and Benefits of Process Safety Management: Industry Survey Results [Journal] // Process Safety Progress. - New York : American Institute of Chemical Engineers, 1994. - 1 : Vol. 13. - pp. 23–29.

Brissaud Florent, Barros Anne and Bérenguer Christophe Probability of Failure on Demand of Safety Systems: Impact of Partial Test Distribution [Journal] // Journal of Risk and Reliability. - 2012. - 4 : Vol. 226. - pp. 426–436.

Cacuci Dan G Sensitivity and Uncertainty Analysis: Theory [Book]. Chapman and Hall/CRC, 2003. - 1st : Vol. 1.

Cantarella J Treatement of Multiple Related Failures by Markov Method [Conference] // Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment. - Ispra : Kluwer Academic Publishers, 1989. - pp. 145-157.

CCF Parameter Estimations 2010 . U.S. Nuclear Regulatory Commission, 2012.

CCPS Plant Guidelines for Technical Management of Chemical Process Safety [Book]. American Institute of Chemical Engineers, 1992 .

CCPS Process Safety Leading and Lagging Metrics: You don’t Improve What you Don’t Measure. Center for Chemical Process Safety, 2011.

Cheol Kim Man and Smidts Carol S Three Suggestions on the Definition of Terms for the Safety and Reliability Analysis of Digital Systems [Journal] // Reliability Engineering and System Safety. - 2015. - Vol. 135. - pp. 81-91.

Confalonieri R, Bellocchi G, Bregaglio S, Donatelli M and Acutis M Comparison of Sensitivity Analysis Techniques: A Case Study with the Rice Model WARM [Journal] // Ecological Modelling. - 2010. - 16 : Vol. 221. - pp. 1897–1906.

Cooper J. Arlin, Ferson Scott and Ginzburg Lev Hybrid Processing of Stochastic and Subjective Uncertainty Data. Sandia National Laboratories, 1995.

Crowl Daniel A and Louvar Joseph F Chemical Process Safety: Fundamentals with Applications [Book]. Prentice Hall International Series in the Physical and Chemical Engineering Sciences, 2011. - 3rd edition.

CSB Investigation Report: Refinery Explosion and Fire. U.S. Chemical Safety and Hazard Investigation Board, 2007.

Cukier R I, Levine H B and Shuler K E Nonlinear Sensitivity Analysis of Multiparameter Model Systems [Journal] // Journal of Computational Physics. - 1978. - 1 : Vol. 26. - pp. 1-42.

Da-Veiga Sébastien Analyse d'incertitudes et de Sensibilité. Application aux Modèles de Cinétique Chimique [Ph.D Dissertation]. Université Toulouse III - Paul Sabatier, 2007.

Dempster A P Upper and Lower Probabilities Induced by a Multivalued Mapping [Journal] // The Annals of Mathematical Statistics. - 1967. - 2 : Vol. 38. - pp. 325–39.

Dhillon B S Maintainability, Maintenance, and Reliability for Engineers [Book]. Taylor & Francis Group, 2006.

Dubois Didier and Prade Henri On the Combination of Evidence in Various Mathematical Frameworks [Book Section] / book auth. Analysis Reliability Data Collection and. - Brussels and Luxembourg : ECSC, EEC, EAEC, 1992.

Durga Rao K, Kushwaha H S, Verma A K and Srividya A Quantification of Epistemic and Aleatory Uncertainties in Level-1 Probabilistic Safety Assessment Studies [Journal] // Reliability Engineering and System Safety. - 2007. - 7 : Vol. 92. - pp. 947–956.

Dutuit Y and Rauzy A Approximate Estimation of System Reliability via Fault Trees [Journal] // Reliability Engineering and System Safety. - 2005. - 2 : Vol. 87. - pp. 163–172.

Dutuit Yves, Innal Fares and Deconinck Geert Etude Complémentaire des Systèmes Instrumentés de Sécurité. Total, 2009.

EN 13306 Maintenance - Maintenance terminology. European Standard, 2010.

EPA QA/G-5S Guidance on Choosing a Sampling Design for Environmental Data Collection. - Washington, DC : U.S. Environmental Protection Agency, 2002.

EPRI Guideline for the Treatment of Uncertainty in Risk-Informed Applications. - California : Electric Power Research Institute, 2006.

Evans M G K, Parry G W and Wreathall J On the treatment of common-cause failures in system analysis [Journal] // Reliability Engineering. - 1984. - 2 : Vol. 9. - pp. 107–115.

Feller William An Introduction to Probability Theory and Its Applications [Book]. Wiley, 1968. - 3rd Edition : Vol. 1.

Ferson S, Hajagos j and Tucker WT Probability Bounds Analysis Is a Global Sensitivity Analysis. Los Alamos National Laboratory, 2005.

Ferson Scott and Hajagos Janos G Arithmetic with Uncertain Numbers: Rigorous and (often) Best Possible Answers [Journal] // Reliability Engineering and System Safety. - 2004. - 1-3 : Vol. 85. - pp. 135–152.

Ferson Scott and Tucker Troy W (a) Sensitivity Analysis Using Probability Bounding [Journal] // Reliability Engineering and System Safety. - 2006. - Vol. 91. - pp. 1435–1442.

Ferson Scott and Tucker Troy W (b) Sensitivity in Risk Analyses with Uncertain Numbers // SAND2006-2801. - Albuquerque : Sandia National Laboratories, 2006.

Ferson Scott Model Uncertainty in Risk Analysis. - 2014. http://rec2014.iit.edu/papers/Paper_Ferson.pdf.

Ferson Scott Naive Monte Carlo Methods Yield Dangerous Underestimates of Tail Probabilities [Conference] // Proceedings of the High Consequence Operations Safety Symposium. - New Mexico : Sandia National Laboratories, 1994.

Ferson Scott RAMAS Risk Calc 4.0 [Software] // Risk Assessment with Uncertain Numbers. Boca Raton, FL: Lewis Publishers, 2002.

Ferson Scott, Ginzburg Lev and Akçakaya Resit Whereof one cannot speak: When input distributions are unknown. - 1996.

Finetti Bruno Theory of Probability: A Critical Introductory Treatment (Wiley Series in Probability and Mathematical Statistics) [Book]. - New York : Wiley, 1975.

Finkelstein Maxim Failure Rate Modelling for Reliability and Risk [Book]. Springer-Verlag, 2008.

Fleming K. N A Reliability Model for Common Mode Failure in Redundant Safety Sytems [Conference] // Proceedings of the Sixth Annua 1 Pittsburgh Conference on Modeling and Simulation. General Atomic Report GA-A13284, 1975.

Fleming K. N and Kalinowski A M An Extension of the Beta Factor Method to Systems wi th High Leve 1 s of Redundancy. Pickard, Lowe and Garrick, 1983.

Fleming K. N and Mosleh A Classification and analysis of reactor operating experience involving dependent events [Book]. Electric Power Research Institute, 1985.

Frank M J, Nelsen R B and Schweizer B Best-possible Bounds for the Distribution of a Sum - Problem of Kolmogorov [Journal] // Probability Theory and Related Fields. - 1987. - 2 : Vol. 47. - pp. 199-211.

Frey Christopher H and Patil Sumeet R Identification and Review of Sensitivity Analysis Methods. - 2002. - Vol. 22.

Goble William M and Cheddie Harry Safety Instrumented Systems Verification: Practical Probabilistic Calculation [Book]. ISA-The Instrumentation, Systems, and Automation Society, 2005.

Goble William M Control Systems Safety Evaluation and Reliability [Book]. ISA Resources for Measurement and Control, 2010. - 3rd edition.

Goble William M, Bukowski Julia V and Brombacher A C (a) How Diagnostic Coverage Improves Safety in Programmable Electronic Systems [Journal] // ISA Transactions. - 1998. - 4 : Vol. 36. - pp. 345-350.

Goble William M (b) The Use and Development of Quantitative Reliability and Safety Analysis in New Product Design [Ph.D Dissertation]. Technische Universiteit Eindhoven , 1998.

GRIF Gaphical Interface for Reliability Forecasting. Total, 2014.

GUM Evaluation of Measurement Data — Guide to the Expression of Uncertainty in Measurement. Joint Committee for Guides in Metrology JCGM 100:2008, 2008.

Guth Michael A S A Probabilistic Foundation for Vagueness & Imprecision in Fault-Tree Analysis [Journal] // IEEE Transactions on Reliability. - 1991. - 5 : Vol. 40. - pp. 563 - 571 .

Hamby D M A Review of Techniques for Parameter Sensitivity Analysis of Environmental Models [Journal] // Environmental Monitoring and Assessment. - 1994. - 2 : Vol. 32. - pp. 135-154 .

Han Sang Gil, Yoon Won Hyo and Chang Soon Heung The Trinomial Failure Rate Model for Treating Common [Journal] // Reliability Engineering and System Safety. - 1989. - 2 : Vol. 25. - pp. 131 - 146.

Hayes Keith R Uncertainty and Uncertainty Analysis Methods. - Hobart : CSIRO Mathematics, Informatics and Statistics, 2011.

Helton J C, Johnson J D, Oberkampf W L and Sallaberry C J Representation of Analysis Results Involving Aleatory and Epistemic Uncertainty. Sandia National Laboratories, 2008.

Helton Jon C, Johnson Jay D and Sallaberry Cédric J Quantification of Margins and Uncertainties: Example Analyses from Reactor Safety and Radioactive Waste Disposal Involving the Separation of Aleatory and Epistemic Uncertainty [Journal] // Reliability Engineering and System Safety. - 2011. - 9 : Vol. 96. - pp. 1014–1033.

Hokstad Per and Corneliussen Kjell Loss of safety assessment and the IEC 61508 standard [Journal] // Reliability Engineering and System Safety. - 2004. - Vol. 83. - pp. 111–120.

Hokstad Per and Corneliussen Kjell Reliability Prediction Method for Safety Instrumented Systems PDS Method Handbook. - Trondheim : SINTEF Industrial Management Safety and Reliability, 2003.

Hokstad Per Common Cause and Dependent Failure Modeling [Book Section] // New Trends in System Reliability Evaluation. - Amsterdam : K.B. Misra, 1993.

Hokstad Per, Maria Alexandre and Tomis Pierre Estimation of Common Cause Factors From Systems With Different Numbers of Channels [Journal] // IEEE Tansictions on Relaibility. - 2006. - 1 : Vol. 55. - pp. 18 - 25.

Homma T and Saltelli A Global Sensitivity Analysis of Nonlinear Models Importance Measures and Sobol' Sensitivity Indices // Report EUR 16052 EN. - Brussels : Joint Research Centre, European Commission , 1994.

Homma Toshimitsu and Saitelli Andrea Importance Measures in Global Sensitivity Analysis of Nonlinear Models [Journal] // Reliability Engineering and System Safety. - 1996. - 1 : Vol. 52. - pp. 1-17.

IAEA Best Estimate Safety Analysis for Nuclear Power Plants: Uncertainty Evaluation // Safety Reports Series 52 . International Atomic Energy Agency, 2008.

IAPA Glossary of Occupational Health & Safety Terms. Industrial Accident Prevention Association, 2007.

IEC 60050 International Electrotechnical Vocabulary // Chapter 191: Dependability and quality of service. International Electrotechnical Commission, 1999.

IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems. - Geneva : International Electrotechnical Commission, 1998.

IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems. - Geneva : International Electrotechnical Commission, 2010.

IEC 61511 Functional Safety – Safety Instrumented Systems for the Process Industry Sector. - Geneva : International Electrotechnical Commission, 2003.

IEC 62278 Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS). International Electrotechnical Commission, 2002.

INERIS – DRA Formalisation du Savoir et des Outils dans le Domaine des Risques Majeurs // L'étude de Dangers d'une Installation Classée (Omega-9). Ministère de l'Ecologie et du Développement Durable (MEDD), 4 10, 2006.

Innal F, Dutuit Y, Rauzy A and Signoret J P New Insight into the Average Probability of Failure on Demand and the Probability of Dangerous Failure per Hour of Safety Instrumented Systems [Journal] // Journal of Risk and Reliability. - 2010. - 2 : Vol. 224. - pp. 75–86.

Innal Fares Contribution à la Modélisation des Systèmes Instrumentés de Sécurité et à l'évaluation de eurs Performances - Analyse critique de la norme CEI 61508 [Ph.D dissertation]. University of Bordeaux 1, 2008.

Innal Fares, Dutuit Yves and Chebila Mourad Safety and Operational Integrity Evaluation and Design Optimisation of Safety Instrumented Systems [Journal] // Journal of Reliability Engineering and System Safety. - 2015. - Vol. 134. - pp. 32-50.

ISA-TR84.00.02-2002 Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques. ISA —The Instrumentation, Systems, and Automation Society, 2002.

ISO 3534-1 Statistics - Vocabulary and Symbols // Part 1: General Statistical Terms and Terms Used in Probability. International Organization for Standardization, 2006.

JCGM Evaluation of Measurement Data - Supplement 1 to the "Guide to the Expression of Uncertainty in Measurement"- Propagation of Distributions Using a Monte Carlo Method. Joint Committee for Guides in Metrology, 2008.

Jin Hui and Rausand Marvin Reliability of Safety-instrumented Systems Subject to Partial Testing and Common-cause Failures [Journal] // Reliability Engineering and System Safety. - 2014. - Vol. 121. - pp. 146–151.

Jin Hui, Lundteigen Mary Ann and Rausand Marvin New PFH-formulas for k-out-of-n:F-systems [Journal] // Reliability Engineering and System Safety. - 2013. - Vol. 111. - pp. 112–118.

Jin Hui, Lundteigen Mary Ann and Rausand Marvin Uncertainty Assessment of Reliability Estimates for Safety-instrumented Systems [Journal] // Journal of Risk and Reliability. - 2012. - 6 : Vol. 226. - pp. 646-655.

JORA Décret exécutif n° 06-198 du 4 Joumada El Oula 1427 correspondant au 31 mai 2006 définissant la réglementation applicable aux établissements classés pour la protection de l'environnement // Journal officiel de la république algérienne. - 6 4, 2006.

JORA Décret exécutif n° 07-144 du 2 Joumada El Oula 1428 correspondant au 19 mai 2007 fixant la nomenclature des installations classées pour la protection de l'environnement // Journal Officiel de la République Algérienne. - 5 22, 2007.

JORA Loi n° 04-20 du 13 Dhou El Kaada 1425 correspondant au 25 décembre 2004 relative à la prévention des risques majeurs et à la gestion des catastrophes dans le cadre du développement durable // Journal Officiel de la République Algérienne. - 12 29, 2004.

Jouffe Lionel and Munteanu Paul BayesiaLab 5.3. - 2010. - http://www.bayesia.com/en/products/bayesialab.php.

JRC-ISIS-SAIE-UASA Evaluation of Sensitivity and Uncertainty Analysis Methods in a Quality Assessment Framework with Application to Environmental and Business Statistics. - Ispra : Joint Research Centre, European Commission, 1999.

Kaufmann A Hybrid Data – Various Associations Between Fuzzy Subsets and Random Variables [Book Section] // Fuzzy Sets Theory and Applications. Springer, 1986. - Vol. 177.

Kendall M G A new measure of rank correlation [Journal] // Biometrika. - 1938. - 1-2 : Vol. 30. - pp. 81-93.

Kiureghian Armen Der and Ditlevsen Ove Aleatory or epistemic? Does it matter? [Journal] // Structural Safety. - 2009. - 2 : Vol. 31. - pp. 105–112.

Klir George and Wierman Mark Uncertainty-Based Information: Elements of Generalized Information Theory (Studies in Fuzziness and Soft Computing) [Book]. Springer-Verlag, 1999.

Kolmogorov A N Foundations of the Theory of Probability [Book]. - New York : Chelsea Pub. Co, 1956.

Langeron Yves, Barros Anne, Grall Antoine and Bérenguer Christophe Safe failures impact on Safety Instrumented Systems [Conference] // European Safety and Reliability Conference- ESREL. - Stavanger, 2007. - pp. 641-648 .

Laprie Jean Claude (a) Dependable Computing and Fault Tolerance: Concepts and Terminology [Conference] // Twenty-Fifth International Symposium on Fault-Tolerant Computing, Highlights from Twenty-Five Years. IEEE, 1995.

Laprie Jean Claude (b) Dependability of Computer Systems: Concepts, Limits, Improvements [Conference] // Sixth International Symposium on Software Reliability Engineering. IEEE , 1995.

Lundteigen Mary Ann and Rausand Marvin Architectural constraints in IEC 61508: Do they have the intended effect? [Journal] // Reliability Engineering and System Safety. - 2009. - 2 : Vol. 94. - pp. 520–525.

Lundteigen Mary Ann and Rausand Marvin (a) Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas [Journal] // Reliability Engineering and System Safety. - 2008. - 8 : Vol. 93. - pp. 1208–1217.

Lundteigen Mary Ann and Rausand Marvin (b) Partial stroke testing of process shutdown valves: How to determine the test coverage [Journal] // Journal of Loss Prevention in the Process Industries. - 2008. - 6 : Vol. 21. - pp. 579–588.

Mannan Sam Lee's Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control [Book]. Elsevier Butterworth-Heinemann, 2005.

Martinez Felipe Aguirre Reliability Analysis of Systems Using Belief Functions Theory to Represent Epistemic Uncertainty [Ph.D Dissertation]. Université de Technologie de Compiègne, 2012.

MATLAB . The Math Works, Int, 2009.

Mazzilli Naomi Sensibilité et Incertitude de Modélisation sur les Bassins Versants à Forte Composante Karstique [Ph.D Dissertation]. Université Montpellier 2, 2011.

McGrath James E Techniques for efficient Monte Carlo simulation [Book]. - Irving, 1975.

McKay M D, Beckman R J and J Conover W Comparison of Three Methods for Selecting Values of Input Variables in the Analysis of Output from a Computer Code [Journal] // Technometrics . - 1979. - 2 : Vol. 21. - pp. 239-245.

Mechri Walid Evaluation de la Performance des Systèmes Instrumentés de Sécurité à Paramètres Imprécis [Ph.D dissertation]. University of Tunis El Manar, 2011.

MIL-STD-721C Military Standard: Definitions of Terms for Reliability and Maintainability. - Washington, DC : Department of Defense (U.S.), 1981.

MIL-STD-882D Standard Practice for System Safety. Department of Defense (U.S.), 2000.

Mokhtari Amirhossein and Frey Christopher H Review and Recommendation of Methods for Sensitivity and Uncertainty Analysis for the Stochastic Human Exposure and Dose Simulation (SHEDS) Models // Volume 1: Review of Available Methods for Conducting Sensitivity and Uncertainty Analysis in Probabilistic Models. - Raleigh, NC : North Carolina State University, 2005.

Morris Max D Factorial Sampling Plans for Preliminary Computational Experiments [Journal] // Technometrics. - 1991. - 2 : Vol. 33. - pp. 161-174.

Mosleh A and Siu N O A Multi- Parameter , Event- Based Common- Cause Failure Model [Conference] // Proceedings of the Ninth International Conference on Structural Mechanics in Reactor Technology. - Lausanne, 1987.

Mousavi Seyedeh Roghayeh Dempster-Shafer Theory and Modified Rules to Determine Uncertainty in Mineral Prospection [Ph.D Dissertation]. TU Clausthal, 2012.

MSHA Coal Fatalities for 1900 Through 2012 [Online] // U.S. Department of Labor, Mine Safety and Health Administration. - 2013. - http://www.msha.gov/stats/centurystats/coalstats.asp.

National Research Council Evaluation of Quantification of Margins and Uncertainties Methodology for Assessing and Certifying the Reliability of the Nuclear Stockpile [Book]. - Washington, D.C : The National Academies Press, 2009.

NEA/ CSNI/ R (92) 18 State of the Art of Level-1 PSA Methodology. Nuclear Energy Agency, 1993.

NRC An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk Informed Activities // RG 1.200. - Washington, D.C : U.S. Nuclear Regulatory Commission, 2007.

NRC An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis // Regulatory Guide 1.174. U.S. Nuclear Regulatory Commission , 1998.

NRC An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis // Regulatory Guide 1.174 . - Washington, D.C : U.S. Nuclear Regulatory Commission, 2002.

NUREG/CR- 2098 Common Cause Fault Rates for Pumps. U.S. Nuclear Regulatory Commission, 1983.

NUREG/CR-4780 (2) Procedures for Treating Common Cause Failures in Safety and Reliability Studies. - Washington, DC : U.S. Nuclear Regulatory Commission ; Electric Power Research Institute, 1989. - Vol. 2.

NUREG/CR-4780 Procedures for Treating Common Cause Failures in Safety and Reliability Studies. - Washington, DC : U.S. Nuclear Regulatory Commission . Electric Power Research Institute, 1988.

NUREG/CR-6819 Common-Cause Failure Event Insights. - Washington, DC : U.S. Nuclear Regulatory Commission, 2003.

NUREG-1855 Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making. U.S. Nuclear Regulatory Commission , 2009.

OJ Council Directive 82/501/EEC on the Major-Accident Hazards of Hertain Industrial Activities. - 1982.

OJEC Council Directive of 96/82/EC of 9 December 1996 on the Control of Major-Accident Hazards Involving Dangerous Substances // Official Journal of the European Communities. - 1 14, 1997.

OJEU Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the Control of Major-Accident Hazards Involving Dangerous Substances, Amending and Subsequently Repealing Council Directive 96/82/EC // Official Journal of the European Union. - 7 24, 2012.

Oliveira Luiz Fernando and Abramovitch Rafael Nelson Extension of ISA TR84.00.02 PFD Equations to KooN Architectures [Journal] // Reliability Engineering and System Safety. - 2010. - 7 : Vol. 95. - pp. 707–715.

Oliveira Luiz Fernando S PFD of Higher-order Configurations of SIS with Partial Stroke Testing Capability // Safety, Reliability and Risk Analysis: Theory, Methods and Applications. Taylor & Francis Group, 2009.

Pannell David J Sensitivity Analysis of Normative Economic Models: Theoretical Framework and Practical Strategies [Journal] // Agricultural Economics. - 1997. - 2 : Vol. 16. - pp. 139–152.

Paredis C J J and Bruns M Numerical Methods for Propagating Imprecise Uncertainty [Conference] // ASME 2006 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. - Pennsylvania, 2006. - Vol. 1.

Parry Gareth W Incompleteness in Data Bases: Impact on Parameter Estimation Uncertainty [Book Section] // Uncertainty in Risk Assessment, Risk Management, and Decision Making. Springer US, 1987. - Vol. 4.

PDS Reliability Prediction Method for Safety Instrumented Systems // PDS Data Handbook. SINTEF, 2010.

PDS Reliability Prediction Method for Safety Instrumented Systems // PDS method handbook. SINTEF, 2006.

R Software R Development Core Team // A Language and Environment for Statistical Computing. - Vienna : R Foundation for Statistical Computing, 2014. - http://www.r-project.org/.

Rakowsky Uwe Kay Fundamentals of the Dempster-Shafer Theory and its Applications to System Safety and Reliability Modelling [Journal] // International Journal of Reliability, Quality and Safety Engineering. - 2007. - 6 : Vol. 14.

Rogers Austin and Milenkovic Aleksandar Security extensions for integrity and confidentiality in embedded processors [Journal] // Microprocessors and Microsystems. - 2009. - Vol. 33. - pp. 398–414.

Rouvroye Johannes L Enhanced Markov Analysis as a Method to Assess Safty in the Process Industry [Ph.D dissertation]. - Eindhoven : Technische Universiteit , 2001.

Sallak Mohamed Evaluation de Paramètres de Sûreté de Fonctionnement en Présence d'incertitudes et Aide à la Conception : Application aux Systèmes Instrumentés de Sécurité [Ph.D dissertation]. - Nancy : Nancy Université, 2007.

Saltelli A, Tarantola S and Chan K P-S A Quantitative Model-Independent Method for Global Sensitivity Analysis of Model Output [Journal] // Technometrics. - 1999. - 1 : Vol. 41. - pp. 39 - 56 .

Saltelli Andrea Saltelli Andrea, Ratto Marco, Andres Terry, Campolongo Francesca, Cariboni Jessica, Gatelli Debora, Saisana Michaela and Tarantola Stefano Global Sensitivity Analysis: The Primer [Book]. - Chichester : John Wiley & Sons, 2008.

Saltelli Andrea, Tarantola Stefano, Campolongo Francesca and Ratto Marco Sensitivity Analysis in Practice: A Guide to Assessing Scientific Models [Book]. Wiley, 2004. - 1st Edition.

Sentz Kari and Ferson Scott Combination of Evidence in Dempster-Shafer Theory // SAND 2002-0835. - 2002.

Shafer Glenn A Mathematical Theory of Evidence [Book]. Princeton University Press , 1976.

Shooman Martin L Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design [Book]. John Wiley & Sons , Inc, 2002.

Simlab 2.2.1 Simulation Environment for Uncertainty and Sensitivity Analysis. Institute for the Protection and Security of the Citizen, Joint Research Centre, European Commission. - http://simlab.jrc.ec.europa.eu.

Simon Christophe and Weber Philippe (a) Imprecise Reliability by Evidential Networks [Journal]. - Journal of Risk and Reliability, 2009. - 2 : Vol. 223. - pp. 119-131.

Simon Christophe and Weber Philippe (b) Evidential Networks for Reliability Analysis and Performance Evaluation of Systems With Imprecise Knowledge [Journal] // IEEE Transactions on Reliability. - 2009. - 1 : Vol. 58. - pp. 69 - 87 .

Smith David J and Simpson Kenneth G L Functional Safety: A Straightforward Guide to applying IEC 61508 and Related Standards [Book]. Elsevier Butterworth-Heinemann, 2004. - 2nd edition.

Smith David J Reliability, Maintainability and Risk [Book]. Butterworth Heinemann, 2007. - 8e edition.

Sobol I M Global Sensitivity Indices for Nonlinear Mathematical Models and their Monte Carlo Estimates [Journal] // Mathematics and Computers in Simulation. - 2001. - 1-3 : Vol. 55. - pp. 271–280.

Sobol I M Sensitivity Estimates for Nonlinear Mathematical Models [In Russian] [Journal] // Matematicheskoe Modelirovanie. - 1990. - Vol. 2. - pp. 112-118. - Translated in Mathematical Modelling and Computational Experiments (1, 407-414, 1993).

Spearman C The proof and measurement of association between two things [Journal] // American Journal of Psychology. - 1904. - 1 : Vol. 15. - pp. 72-101.

Stamatelatos Michael Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. - Washington, DC : Office of Safety and Mission Assurance NASA Headquarters, 2002.

Summers Angela E Partial Stroke Testing of Block Valves // Instrument Engineers Handbook. SIS-TECH Solutions, 2006. - Vol. 4.

Summers Angela E Safety Instrumented Systems [Book Section] // Perry’s Handbook of Chemical Engineering / book auth. Green Don and Perry Robert. McGraw Hill Professional, 2007. - 8th edition.

Swiler Laura P, Paez Thomas L and Mayes Randall Epistemic Uncertainty Quantification Tutorial [Conference] // Proceedings of the IMAC-XXVII. - Florida : Society for Experimental Mechanics Inc, 2009.

Thunnissen Daniel P Uncertainty Classification for the Design and Development of Complex Systems [Conference] // 3rd Annual Predictive Methods Conference. - California, 2003.

Tiezema R J Risk Reduction in the Process Industry-Proof Testing. - 2003.

Torres-Echeverría A C, Martorell S and Thompson H A Modeling Safety Instrumented Systems with MooN Voting Architectures Addressing System Reconfiguration for Testing [Journal] // Reliability Engineering and System Safety. - 2011. - 5 : Vol. 96. - pp. 545–563.

Villemeur A Sûreté de fonctionnement des systèmes industriels [Book]. Eyrolles, 1988.

VIM International Vocabulary of Metrology – Basic and General Concepts and Associated Terms. - Geneva : International Organization for Standardization, 1993. - 2nd Edition.

Williamson Robert C and Downs Tom Probabilistic Arithmetic. I. Numerical Methods for Calculating Convolutions and Dependency Bounds [Journal] // International Journal of Approximate Reasoning. - 1990. - 2 : Vol. 4. - pp. 89-158.

Wolfgang Velten-Philipp and Houtermans Michel The Fffect of Diagnostic and Periodic Proof Testing on the Availability of Programmable Safety Systems [Conference] // Proceedings of the 10th WSEAS International Conference on Communications. - Athens, 2006. - pp. 180-186.

Wu Fu-Chun and Tsang Yin-Phan Second-order Monte Carlo Uncertainty/variability Analysis Using Correlated Model Parameters: Application to Salmonid Embryo Survival Risk Assessment [Journal] // Ecological Modelling. - 2004. - 3 : Vol. 177.

Xu Ming, Chen Tao and Yang Xianhui The Effect of Parameter Uncertainty on Achieved Safety Integrity of Safety System [Journal] // Reliability Engineering and System Safety. - 2012. - Vol. 99. - pp. 15–23.

Xu Peida, Deng Yong, Su Xiaoyan and Mahadevan Sankaran A New Method to Determine Basic Probability Assignment from Training Data [Journal] // Knowledge-Based Systems. - 2013. - Vol. 46. - pp. 69–80.

Yager Ronald R Arithmetic and Other Operations on Dempster-Shafer Structures [Journal] // International Journal of Man-Machine Studies. - 1986. - 4 : Vol. 25. - pp. 357–366.

Yager Ronald R On the Dempster-Shafer Framework and New Combination Rules [Journal] // Information Sciences. - 1987. - 2 : Vol. 41. - pp. 93–137.

Yang Jianping, Huang Hong-Zhong, Liu Yu and Li Yan-Feng Evidential Networks for Fault Tree Analysis with Imprecise Knowledge [Journal] // International Journal of Turbo & Jet-Engines. - 2012. - 2 : Vol. 29. - pp. 111–122.

Yoshimura Itaru Safety Achieved by the Safe Failure Fraction (SFF) in IEC 61508 [Journal] // IEEE Transaction on Reliability. - 2008. - 4 : Vol. 57. - pp. 662 - 669.

Zadeh L A Fuzzy Sets [Journal] // Information and Control. - 1965. - 3 : Vol. 8. - pp. 338--353.

Zio E and Apostolakis G E Two Methods for the Structured Assessment of Model Uncertainty by Experts in Performance Assessments of Radioactive Waste Repositories [Journal] // Reliability Engineering and System Safety. - 1996. - 2-3 : Vol. 54. - pp. 225–241.

Zio Enrico (a) The Monte Carlo Simulation Method for System Reliability and Risk Analysis [Book]. Springer-Verlag, 2013.

Zio Enrico and Pedroni Nicola (b) Literature Review of Methods for Representing Uncertainty // Les Cahiers de la Sécurité Industrielle. - Toulouse : Foundation for an Industrial Safety Culture, 2013.

Zitrou Athena, Bedford Tim and Walls Lesley An Influence Diagram Extension of the Unified Partial Method for Common Cause Failures [Journal] // Quality Technology & Quantitative Management. - 2007. - 1 : Vol. 4. - pp. 111-128.

Appendix

This appendix is dedicated to describe some of the widely used global sensitivity methods, which could be split into MC based measures and variance based measures.

- **Monte Carlo based approach**

Unquestionably, many of the most commonly used SA methods belong to this Monte Carlo (sampling) based approach. Predominantly, after following the same process of this latter method for the propagation of uncertainties (see section 5.1.3) several correlation, regression and even visual measures could be estimated for the SA.

✓ *Pearson Product-Moment Correlation Coefficient* (*PPMCC* or *PEAR*): Aka correlation coefficient (*CC*) is a number between -1 and 1 that represents the strength of the linear relationship between two variables *X* and *Y*. The values 1 and -1 represent the total positive and negative correlation, while 0 means the absence of any linear relationship between the two variables. Eqs. (6.1) and (6.2) could be used to obtain such coefficient for the populations (ρ) and/or for their samples of *n* observations (r).

$$\rho_{X,Y} = \frac{E(XY) - E(X)E(Y)}{\sqrt{E(X^2) - E^2(X)}\sqrt{E(Y^2) - E^2(Y)}} \tag{6.1}$$

$$r_{x,y} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}} \tag{6.2}$$

where, $E(.)$ denotes the expectation, x_i, y_i are the sampled values for X, Y and $\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$, $\bar{y} = \frac{1}{n}\sum_{i=1}^{n} y_i$ are the samples mean.

✓ *Spearman Rank Correlation Coefficient* (*SPEA*): In purpose of overcoming the limitation of the linearity in the previous coefficient, several alternative solutions have been proposed known as the *non-parametric* techniques like the Spearman's Rank Correlation Coefficient (Spearman, 1904) and Kendall's Rank Correlation Coefficient (Kendall, 1938). The main idea is ranking the values of each variable (undependably) and using those ranks instead of the values. Eq. (6.3) could be used to calculate the *SPEA* when no ties exist (i.e., no two values share the same rank).

$$r_s = 1 - \frac{6\sum_{i=1}^{n} d_i^{\,2}}{n(n^2-1)} \tag{6.3}$$

where, $d_i = R(x_i) - R(y_i)$ is the difference in the ranks of x_i, y_i .

- ✓ *Partial Correlation Coefficient* (*PCC*): This coefficient provides the possibility of identifying the correlation between two variables while eliminating the other variables' effects. For three variables, two inputs X_1, X_2 and an output *Y*, the *PCC* for X_1 and *Y*, where the effects of X_2 are neglected could be computed using Eq. (6.4).

$$r_{X_1Y/X_2} = \frac{r_{X_1Y} - r_{X_1X_2} r_{X_2Y}}{\sqrt{(1-r^2{}_{X_1X_2})(1-r^2{}_{X_2Y})}} \tag{6.4}$$

- ✓ *Partial Rank Correlation Coefficient* (*PRCC*): This is another non-parametric technique that can also be used in presence of a nonlinear but monotonic relationship between the relevant variables.
- ✓ *Standardized Regression Coefficient* (*SRC*): The main idea behind the regression techniques is substituting the complex model with another simple one in form of:

$$Y = \beta_0 + \sum_{j=1}^{p} \beta_p X_p + \varepsilon \tag{6.5}$$

where, Y is the *dependent* variable (response), $X_1, X_2, ..., X_p$ are the *independent* variables (inputs), when *p*=1 we call Eq. (6.5) *simple linear regression model* and when *p*>1 it will be a *multiple linear regression model*. β_0 is the *intercept*, $\beta_1, \beta_2, ..., \beta_p$ are the *slopes* and together they are known as *regression coefficients*, which could be estimated using the *least squares* method. Lastly, ε is the random error term that conventionally has a zero mean. Now, for each observation x_i (*i=1,2,…,n*) of X_j we can get:

$$y_i = \beta_0 + \sum_{j=1}^{p} \beta_j x_{ij} + \varepsilon_i \tag{6.6}$$

From this latter equation we can obtain the *residual sum of squares* (*RSS*):

$$RSS = \sum_{i=1}^{n} \varepsilon_i^2 = \sum_{i=1}^{n} (y_i - \beta_0 - \sum_{j=1}^{p} \beta_j x_{ij})^2 \tag{6.7}$$

The *least squares estimators* $\hat{\beta}_0, \hat{\beta}_1, ..., \hat{\beta}_p$ of $\beta_0, \beta_1, ..., \beta_p$ are the values that minimize the *RSS* with respect to $\hat{\beta}_0, \hat{\beta}_1, ..., \hat{\beta}_p$ as represent Eqs. (6.8) and (6.9):

$$\frac{\partial RSS}{\partial \hat{\beta}_0} = -2\sum_{i=1}^{n} (y_i - \hat{\beta}_0 - \sum_{j=1}^{p} \hat{\beta}_j x_{ij}) = 0 \tag{6.8}$$

$$\frac{\partial RSS}{\partial \hat{\beta}_j} = -2\sum_{i=1}^{n}(y_i - \hat{\beta}_0 - \sum_{j=1}^{p}\hat{\beta}_j x_{ij})x_{ij} = 0 \tag{6.9}$$

The simplification of these two equations will yield the following set of *p*+1 *normal* equations:

$$\begin{aligned}
&n\hat{\beta}_0 + \hat{\beta}_1\sum_{i=1}^{n}x_{i1} + ... + \hat{\beta}_p\sum_{i=1}^{n}x_{ip} = \sum_{i=1}^{n}y_i \\
&\hat{\beta}_0\sum_{i=1}^{n}x_{i1} + \hat{\beta}_1\sum_{i=1}^{n}x_{i1}x_{i1} + ... + \hat{\beta}_p\sum_{i=1}^{n}x_{i1}x_{ip} = \sum_{i=1}^{n}x_{i1}y_i \\
&\qquad\qquad\cdots\cdots \\
&\hat{\beta}_0\sum_{i=1}^{n}x_{ip} + \hat{\beta}_1\sum_{i=1}^{n}x_{ip}x_{i1} + ... + \hat{\beta}_p\sum_{i=1}^{n}x_{ip}x_{ip} = \sum_{i=1}^{n}x_{ip}y_i
\end{aligned} \tag{6.10}$$

By solving Eq. (6.10), we can find $\hat{\beta}_0, \hat{\beta}_1, ..., \hat{\beta}_p$, and then we can write Eq. (6.6) as:

$$y_i = \hat{y}_i + e_i = \hat{\beta}_0 + \sum_{j=1}^{p}\hat{\beta}_j x_{ij} + e_i \tag{6.11}$$

where, $\hat{y}_i$ is the estimator of y_i and it is obvious that e_i is the difference between the response's observed and estimated values or the *residual*.

By standardizing $\hat{y}_i$ we find:

$$\frac{(\hat{y}_i - \bar{y})}{\hat{s}} = \sum_{j=1}^{p}(\frac{\hat{\beta}_j\hat{s}_j}{\hat{s}})\frac{(x_{ij} - \bar{x}_j)}{\hat{s}_j} \tag{6.12}$$

where, $\hat{s} = \sqrt{\sum_{i=1}^{n}\frac{(y_i - \bar{y})}{n-1}}$ and $\hat{s}_j = \sqrt{\sum_{i=1}^{n}\frac{(x_i - \bar{x})}{n-1}}$ are the standard deviations of the dependent and independent variables respectively. Moreover, the term $\frac{\hat{\beta}_j\hat{s}_j}{\hat{s}}$ is the standardized regression coefficient (*SRC*), what allows us to express Eq. (6.12) as:

$$\frac{(\hat{y}_i - \bar{y})}{\hat{s}} = \sum_{j=1}^{p}SRC(x_j - \bar{x}_j)/\hat{s}_j \tag{6.13}$$

Supposing that the input variables are independent and the regression model is acceptably represents the actual data (use the *coefficient of multiple determination R^2*), the *SRC* could be used as a sensitivity measure.

- ✓ *Standardized Rank Regression Coefficient* (*SRRC*): Once again, the linearity problem can be overcome by using the ranks instead of the real values, but exactly as *SPEA* and PRCC the monotonic trait always remain required.

- **Variance based approach**

Without being concerned about the nature of the relationship between the inputs and the output (s), this approach seeks to assess the contribution of each input factor represented by its variance on the total variance of the output. Usually, the computation cost is the weakest point of such methods but for a small number of inputs this approach is highly recommended.

✓ *Sobol' sensitivity indices*: Its exhaustive description is provided in (Sobol, 1990; Sobol, 2001) but in brief, let us assume that a given model is represented by the following function:

$$Y = f(X_1, X_2, ..., X_p) \tag{6.14}$$

where, Y is the model output and $X = (X_1, X_2, ..., X_p)$ are the inputs that are considered independent and uniformly distributed in the unit hypercube.

Let the Eq. (6.15) to be the ANOVA-representation of $f(X)$, which is a summation of 2^p terms of *increasing dimensionality* (Sobol, 2001):

$$Y = f(X) = f_0 + \sum_{s=1}^{p} \sum_{j_1<...<j_s}^{p} f_{j_1 \cdots j_s}(X_{j_1}, ..., X_{j_s}) \tag{6.15}$$

where $1 \le j_1 < ... < j_s \le p$, and f_0 is a constant.

This latter formula can be rewritten as:

$$\int f^2(X)dX - f_0{}^2 = \sum_{s=1}^{p} \sum_{j_1<...<j_s}^{p} \int f_{j_1 \cdots j_s}^2 dX_{j_1} ... dX_{j_s} \tag{6.16}$$

In fact, Eq. (6.16) means that:

$$V = \sum_{s=1}^{p} \sum_{j_1<...<j_s}^{p} V_{j_1 \cdots j_s} \tag{6.17}$$

where, V is the variance of Y, and $V_{j_1 \cdots j_s}$ are the variances of the summands in Eq. (6.15) respectively and the multidimensional integrals in Eq. (6.16) are usually estimated by MC methods.

The global sensitivity indices are:

$$S_{j_1, j_2, ..., j_S} = \frac{V_{j_1, j_2, ..., j_S}}{V} \tag{6.18}$$

where, the small *s* is called the index's order (dimension).

To directly (using one integral) get the total effect sensitivity index S_{T_j} of X_j that includes the fraction of variance accounted for by X_j alone and the fraction accounted for by any combination of X_j with the remaining variables, it has been suggested in (Homma, et al., 1994; Homma, et al., 1996) and to use the following equation:

$$S_{T_j} = 1 - S_{cj} \tag{6.19}$$

where S_{cj} equals the sum of all the $S_{j_1, j_2, ..., j_S}$ terms where the index j is excluded.

✓ *Fourier Amplitude Sensitivity Test* (*FAST*): This method that was introduced in (Cukier, et al., 1978) proceeds by relating the probability distribution of each parameter to a frequency ω_j and a new parameter (scalar variable) *s* where, as *s* varies, carries all the parameters through their range of variation. Let us retain the same model presented by Eq. (6.14), the key idea of this method is employing the following transformation in purpose of converting the multidimensional integral into one-dimensional one:

$$X_j = G_j(\sin \omega_j s), \qquad \forall j = 1,2,..., p \tag{6.20}$$

where, G_j are called transformation functions that should be duly defined, ω_j are a set of incommensurate frequencies assigned arbitrarily for X_j, and the *search variable s* varies from $-\infty$ to ∞.

Performing the Fourier analysis, the output variance could be expressed as:

$$V \approx \frac{1}{2} \sum_{k=1}^{\infty} (A_k^2 + B_k^2) \tag{6.21}$$

where A_k and B_k are the Fourier coefficients that are defined as:

$$A_k = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(s) \cos(ks) ds,$$

$$B_k = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(s) \sin(ks) ds \tag{6.22}$$

The partial variances are approximated as:

$$V_j \approx \frac{1}{2} \sum_{h=1}^{\infty} (A_{h\omega_j}^2 + B_{h\omega_j}^2) \tag{6.23}$$

where, A_{ω_j} and B_{ω_j} are the Fourier coefficients of the fundamental frequency ω_j and all of its harmonics ($h = 1,2,...$).

By obtaining the output variance and the partial variances, the identification of the main effect could be estimated in the same manner as in the sobol' technique (i.e., computing the ratio represented by Eq. (6.18)). The extended Fourier Amplitude Sensitivity Test (*eFAST*) has been proposed in (Saltelli, et al., 1999) to provide the ability to estimate the total (all effects) contribution of each factor to the output variance.